State of the ATT&CK

Blake Strom
@stromcoffee

@MITREattack

#ATTACKcon

MITRE

ATT&CK Circa 2014

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	OS/Software Weakness	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration		Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration		Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit			Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				
AT / Schtasks / Cron			File system enumeration				

Detect	Partially Detect	No Detect	No Usage

ATT&CK To

ATT&CK Sightings

ATT&CK Evaluations

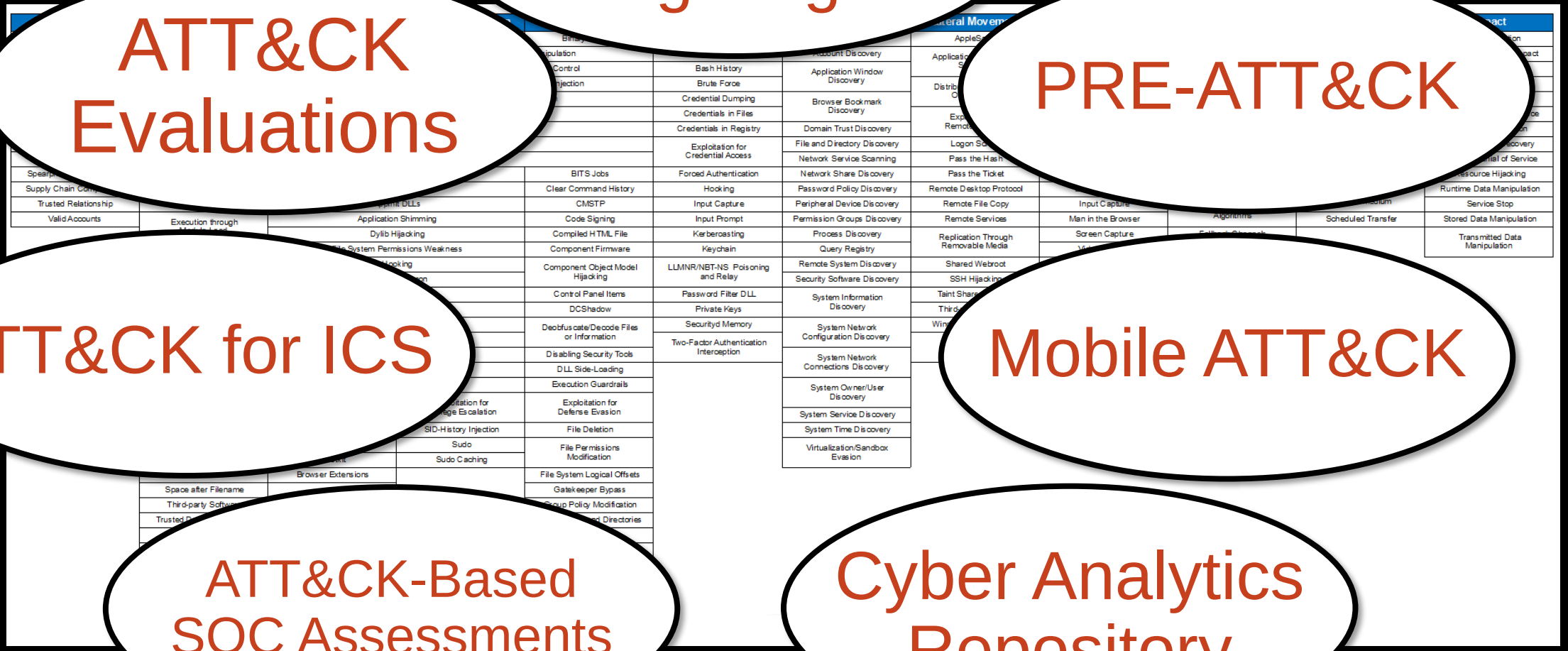
PRE-ATT&CK

ATT&CK for ICS

Mobile ATT&CK

ATT&CK-Based SOC Assessments

Cyber Analytics Repository



We Didn't Get Here By Accident

ATT&CK™

MITRE

Updates this Year – By the Numbers

1 NEW TACTIC

43 NEW TECHNIQUES

13 NEW MOBILE TECHNIQUES

16 NEW GROUPS

87 NEW SOFTWARE

41 NEW MITIGATIONS

87 UPDATED TECHNIQUES

16 UPDATED MOB TECHNIQUES

67 UPDATED GROUPS

92 UPDATED SOFTWARE

ATT&CK™

MITRE

MITRE | ATT&CK™ for Cloud

Credit to Dave Herrald and Ryan Kovar

ATT&CK for Cloud

- **36 techniques**
- **Part of Enterprise ATT&CK**
- **Almost 100% community-contributed techniques!**
  - Input from:
    - A cloud service provider
    - Red teams
    - Threat analysts
    - Detection analysts

Google Cloud

ATT&CK™

MITRE

Impact Tactic

- Attacks targeting availability and integrity
  - Ex: Ransomware, DoS, destruction
- 16 techniques

Data Destruction	Endpoint DoS	Resource Hijacking	Runtime Data Manipulation
Data Encrypted for Impact	Network DoS	Service Stop	Stored Data Manipulation
Disk Content Wipe	Firmware Corruption	Defacement	Transmitted Data Manipulation
Disk Structure Wipe	Inhibit System Recovery	New! System Shutdown/Reboot	New! Account Access Removal

Mitigations

Home > Techniques > Enterprise > Spearphishing Attachment

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

MITRE

Abstraction Issues in ATT&CK

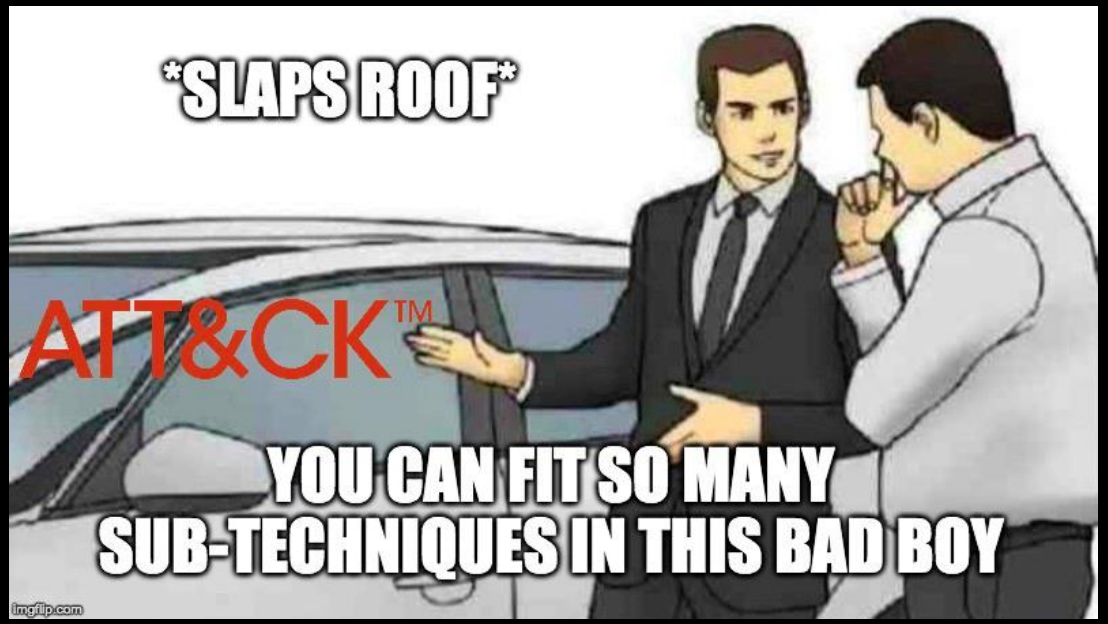
- **Some broad techniques**
  - Account Manipulation
  - Credential Dumping
- **Some narrow**
  - Rundll32
  - MSBuild
- **Hard to strike the right balance now**

How Do We Scope Sub-Techniques?

- Groups of behaviors
- Use what we have
- Maintain an adversary mindset
- Platform specific techniques

Sub-Technique Implementation

- **Rough stats (so far)**
  - Techniques: 266 ➡ 166
  - Sub-techniques: 280
- **Implementing now**
  - Pausing other updates
  - No groups/software!
- **Going into companion website for preview**
  - Won't be defacto ATT&CK
  - 3+ month feedback period



Sub-Technique Example

Credential Access
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
…

Credential Dumping Sub-Techniques (draft)
SAM (Security Accounts Manager)
Local Security Authority (LSA) Secrets
NTDS from Domain Controller
Cached Credentials
…

Sub-Technique Feedback

- **Are sub-techniques necessary and are we on the right track?**
  - Overwhelmingly, yes!
- **Aren't they procedures?**
  - No
- **Visualization challenges**
- **One-to-many issues**
- **Mapping old to new**
- **Data source refinement**
- **OS agnostic techniques**
- **Techniques should always have sub-techniques**
- **Sub-techniques should be OS specific**
- **Will help with false sense of security**

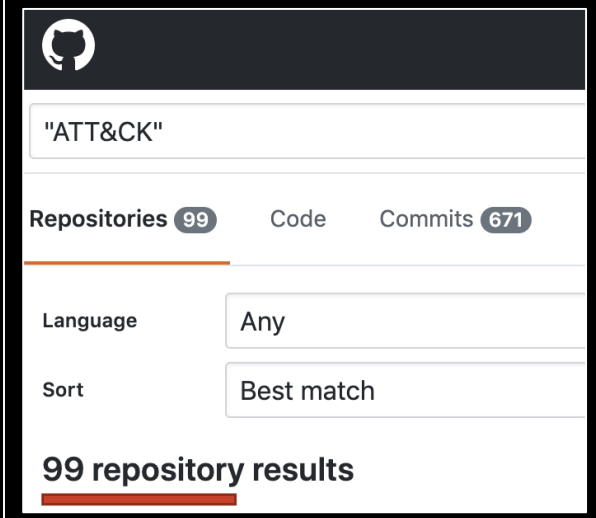
ATT&CK™

MITRE

Growth of the ATT&CK Community

Individuals + orgs contributing to ATT&CK!

- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Alex Hinchliffe, Palo Alto Networks
- Alfredo Abarca
- Allen DeRyke, ICE
- Anastasios Pingios
- Andrew Smith, @jakx_
- Avneet Singh
- Barry Shteiman, Exabeam
- Bart Parys
- Bartosz Jerzman
- Brian Prange
- Bryan Lee
- Carlos Borges, @huntingneo, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Christoffer Strömblad
- Cody Thomas, SpecterOps
- Craig Aitchison
- CrowdStrike Falcon OverWatch
- Cybereason Nocturnus, @nocturnus
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Drew Church, Splunk
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, CYBINT Centre
- Elia Florio, Microsoft
- Elly Searle, CrowdStrike
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erika Noerenberg, @gutterchurl, Carbon Black
- Erye Hernandez, Palo Alto Networks
- ESET
- Felipe Espósito, @Pr0teus
- Filip Kafka, ESET
- FS-ISAC
- Hans Christoffer Gaardløs
- Heather Linn
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Ivan Sinyakov
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jannie Li, Microsoft (MSTIC)
- Jared Atkinson, @jaredcatkinson
- Jean-Ian Boutin, ESET
- Jeff Sakowicz, Microsoft (IDPM Services)
- Jeremy Galloway
- Jimmy Astle, @AstleJimmy, Carbon Black
- Johann Rehberger
- John Lambert, Microsoft (MSTIC)
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Jörg Abraham, EclecticIQ
- Kaspersky
- Lab52 by S2 Grupo
- Leo Loobeek, @leoloobeek
- Loic Jaquemet
- Lucas da Silva Pereira, @vulcanunsec, CIP
- Lukáš Štefanko, ESET
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Martin Jirkal, ESET
- Martin Smolar, ESET
- Matias Nicolas Porolli, ESET
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Michal Dida, ESET
- Microsoft Threat Intelligence Center (MSTIC)
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Netskope
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Oleg Kolesnikov
- Oleg Skulkin, Group-IB
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM
- Pedro Harrison
- Praetorian
- Prashant Verma, Paladion
- Rahmat Nurfauzi, PT Xynexis International
- Red Canary
- RedHuntLabs, @redhuntlabs
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Rob Smith
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Sahar Shukrun
- Saisha Agrawal, Microsoft (MSTIC)
- Scott Lundgren, @5twenty9, Carbon Black
- Shailesh Tiwary (Indian Army)
- Shane Tully, @securitygypsy
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Swetha Prabakaran, Microsoft (MSTIC)
- Sylvain Gil, Exabeam
- Tatsuya Daitoku, Cyber Defense Institute, Inc.
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Uelтschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Wayne Silva, Countercept
- Ye Yint Min Thu Htut, DBS Bank
- Yonatan Gotlib, Deep Instinct



Things Yet to Come

Mobile ATT&CK
Enterprise ATT&CK
PRE-ATT&CK

It's just ATT&CK™

ICS ATT&CK

Mappings to Controls Frameworks

MITRE

More ATT&CK Updates!

Tuesday

1:30 pm TRAM

3:45 pm ATT&CK Sightings

Wednesday

10:15 am ICS ATT&CK

12:00 pm Controls Mapping

2:00 pm CAR and Analytics

3:15 pm PRE Integration

Blake Strom
@stromcoffee

ATT&CK™

attack@mitre.org
@MITREattack
#ATTACKcon

MITRE