black hat
EUROPE 2018

Real-Time AD Attack Detection: Detect Attacks Leveraging Domain Administrator Privilege

December 6

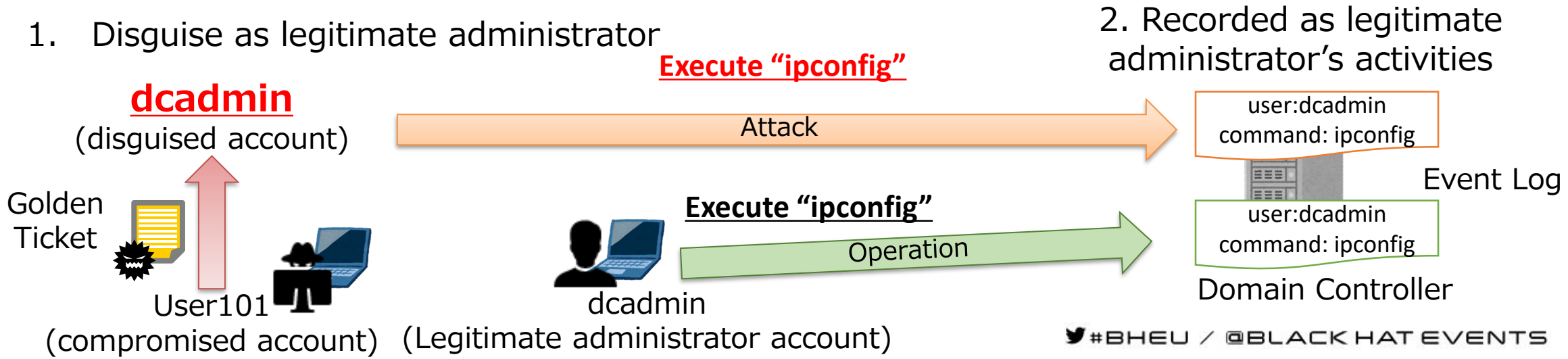
The University of Tokyo
Wataru Matsuda,
Mariko Fujimoto,
Takuho Mitsunaga

Introduction

- In targeted attacks, attackers tend to attack Active Directory (AD) in order to expand infections
- Attackers try to take over **Domain Administrator privileges** and create a backdoor called the "**Golden Ticket**"
- Attackers leverage the Golden Ticket to disguise themselves as **legitimate administrator accounts** to avoid detection **for a long period** of time
- We've implemented a real-time detection tool combining **signature-based** and **machine learning** detection that utilizes **Domain Controller Event Logs** in order to detect attack activities including the use of Golden Tickets

Difficulty of detecting Golden Ticket attacks

- **Golden Ticket** is a Kerberos authentication ticket created by the attackers that has a **legitimate signature** and **a long term of validity** (e.g. ten years)
- Attackers use some **built-in windows commands** in addition to attack tools
- It is difficult to identify attackers' activities if legitimate administrators often use commands in daily operations



Summary of our tool

- We've implemented a real-time detection tool to detect attack activities that abuse Domain Administrator privileges such as the use of Golden Tickets
- It analyzes Event Logs with **signature-based and machine learning detection** to yield high detection rate
- If attackers' activities are detected, real-time alerts are raised

Methods	Advantages	Disadvantages
Signature-based detection	It yields **high recall rate**.	A lot of **false positive** can occur depending on the daily operations.
Machine learning detection	It can find **unusual activities** compared with daily operations.	False negative can occur in some situations.

Signature-based detection

- We pick up several useful existing methods, and organize specific detection signatures

	Signature
A	Monitor unexpected use of administrative privilege using Event ID: 4672
B	Monitor execution of CLI tools that attackers tend to use from Event ID: 4688, 4674
C	Monitor Use of administrative shared resources using Event ID: 5140
D	Service Ticket requests made without a prior TGT request using Event ID: 4768, 4769

Signature B) Execution of tools attackers tend to use

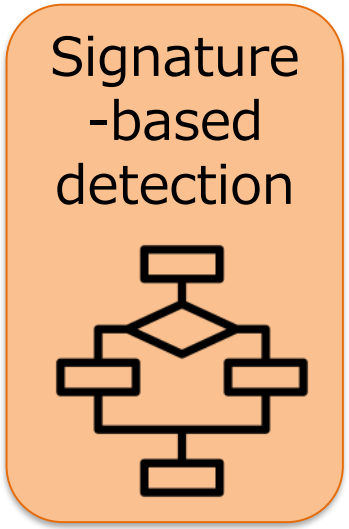
- We register the following commands into the blacklist, since they tend to be used by attackers

Command	
tasklist.exe	type
ver	at.exe
ipconfig.exe	reg.exe
systeminfo.exe	wmic.exe
net.exe	wusa.exe
netstat.exe	netsh.exe
whoami.exe	sc.exe
qprocess.exe	rundll32.exe
query.exe	schtasks.exe
dir	ping.exe

Reference: https://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

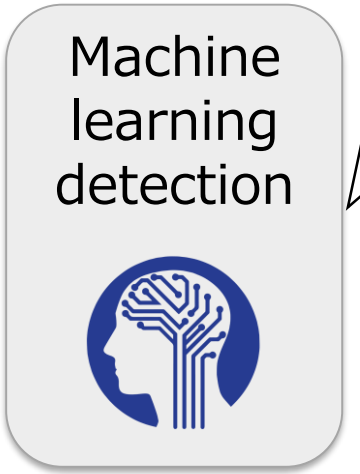
Machine learning detection

- For signature B, a lot of **false positives** can occur when the legitimate Domain Administrator uses the commands included in the blacklist for daily operations
- To solve the problem, we re-analyze the results of signature-based detection using **machine learning**



This is “Attack” since “ipconfig” is on the blacklist.

False positive



This is **not an ”Attack”** since “ipconfig” is used in daily operations.

True Negative

Implementation of our tools

Launch Detection programs

Logstash

Logs are sent in real-time

Winlogbeat (Log transfer agent)

If matches signature A, C or D

Signature-based detection

Domain Controller

Visualize with Kibana

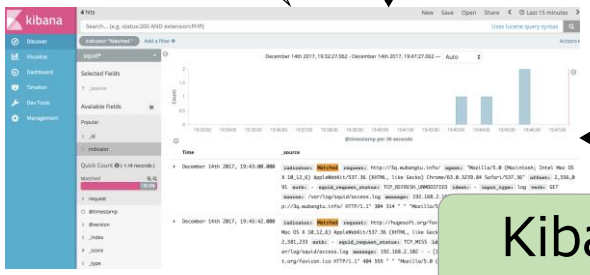
Send alert mail

If matches signature B (suspicious commands)

Machine learning detection

Elastic Search

Preserve logs

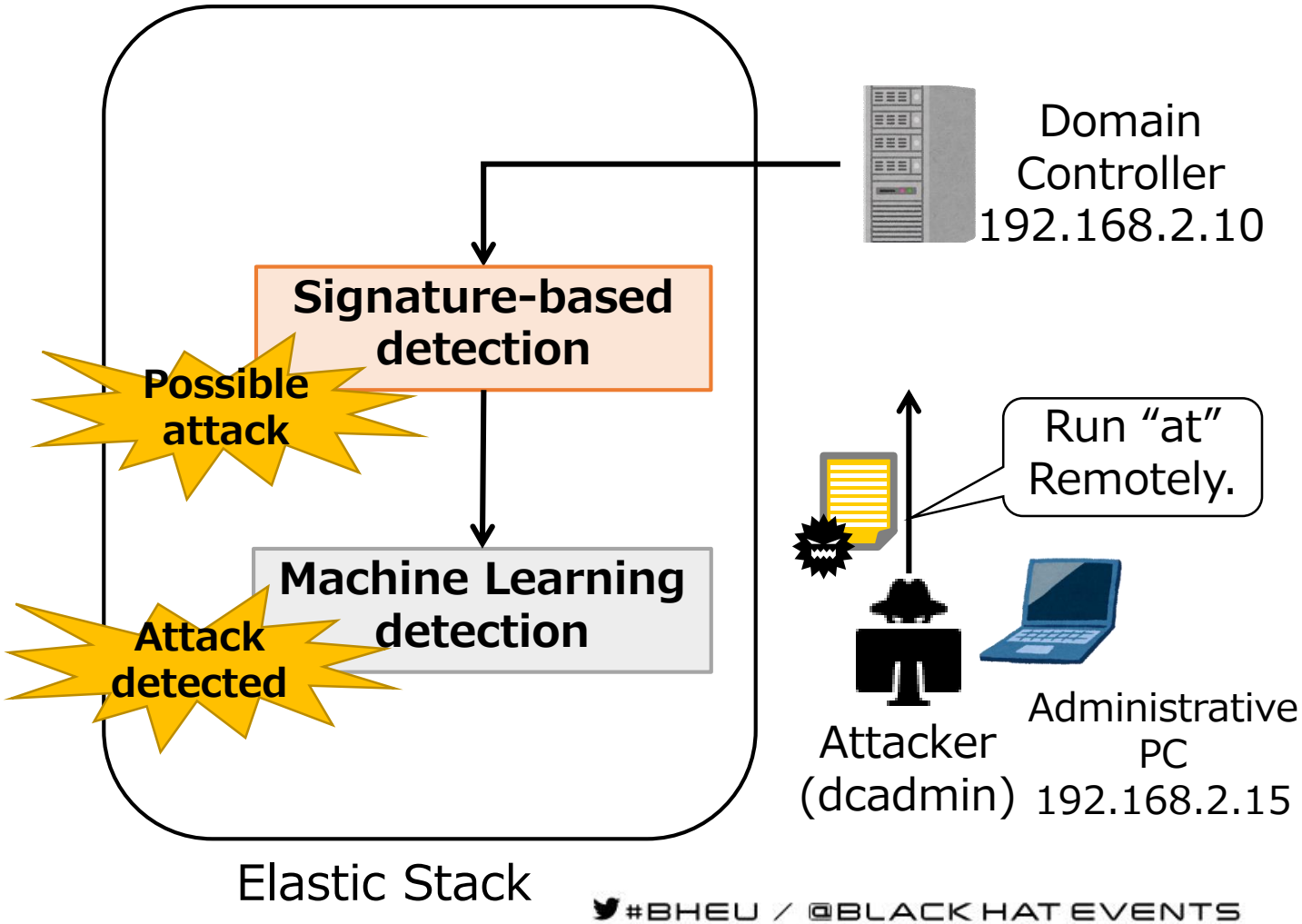


Kibana

Elastic Stack

Demonstration scenario

1. Attacker take over Domain Administrator privilege leveraging **privilege escalation** vulnerability (MS14-068)
2. Create Golden Ticket for dcadmin
3. Accesses the DC using remote access tool "**PsExec**" with a **Golden Ticket** and run **"at" command**
4. Signature-based detection detects attack since "at" is on the blacklist
5. Machine Learning also detects attack since "at" command is not used in daily operations
6. An alert mail is sent to the security administrator



We published the sample code of our tool.

https://github.com/sisoc-tokyo/Real-timeDetectionAD

Thank you for your attention!

coe@sisoc.org