Real-time detection of high-risk attacks leveraging Kerberos and SMB

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

1. Introduction

In Advanced Persistent Threat (APT) attacks, attackers tend to attack against the Active Directory and expand infections. Especially a Remote Code Execution vulnerability fixed in MS14-068 and MS17-010 have been leveraged around the world and attackers can get administrator privileges leveraging the vulnerability. Attackers who can get administrator privileges likely create "Golden Ticket" and ”Silver Ticket” in order to disguise themselves as arbitrary legitimate account for a long period. However, detecting attacks using these methods are quite difficult since they tend to leverage legitimate accounts and processes, which are not identified as anomaly.

In this research, a real-time detection method for the following attack activities using Event logs and Kerberos packets is introduced.

・Attacks leveraging the vulnerability of MS14-068 and MS17-010
・Attacks using Golden Ticket
・Attacks using Silver Ticket

This method utilizes only Domain Controller’s built-in Event Logs and minimum communication packets. Thus it can be implemented relatively in easy way even in case that it is difficult to apply security measures immediately, and helps immediate response to attacks. Additionally, ATT&CK, a knowledge base of adversary tactics and techniques, is getting common recently. We also introduce the method to identify the possible tactics for each detected attack activity automatically.

Our method consists of the following functions in order to reduce false detection rate and help immediate response.

・ **Event Log analysis**

Step1 (Signature-based detection): Event Logs are firstly analyzed with several signatures (signature A, B, C, D) focusing on the characteristics of the attack activities.

Step2 (Machine learning detection or whitelist): Event Logs are further analyzed with machine learning and unusual command execution are detected. White lists can be used

instead of machine learning if the operational environment is relatively stable.

Step3 (Real-time alert): If attack activities are detected, real-time alerts are raised using Elastic Stack.

- **Packet analysis**

Step1 Golden Ticket detection: Find Golden Ticket attacks from Kerberos packets together with Event Log.

Step2 Silver Ticket detection: Find Silver Ticket attacks from Kerberos packets.

Step3 (Real-time alert): If attack activities are detected, real-time alerts are raised using Elastic Stack.

Table 1 shows each whether each function can detect attack activities.

Table 1. Mapping of attack activity and detection function

Attack activity		Event Log analysis	Packet analysis
MS14-068		○	—
MS17-010		○	—
Golden Ticket	A)Unexpected administrative privilege use	○	—
	B)Execution of tools attackers tend to use	○	—
	C)Use of administrative shared resource	○	—
	D)ST requests without a prior TGT request.	○	○ *1
Silver Ticket		×	○

○：Can detect the attack

× : Cannot detect the attack

-: Not use

*1: Not necessary but if use, detection accuracy can be improved

2. Summary of Active Directory

Active Directory (AD) is a centralized management system for Windows computers and accounts. In an AD environment, the main form of authentication that is used is the Kerberos Authentication. In the Kerberos authentication, the DC uniformly processes all authentications, using authentication tickets called Ticket-Granting Tickets (TGT) and Service Tickets (ST).

- Ticket-Granting Tickets (TGT): A ticket that proves the authenticity of the user. The client requests for a TGT to the DC on its first authentication process, and the TGT is stored in the users' machine and repeatedly used until its expiration. The default expiration limit for a ticket is ten hours since the its creation. TGTs (including the Golden Ticket) are signed and encrypted by the password hash (hashed value of the password) of the krbtgt account, which is the built-in service account on the DC.
- Service Ticket (ST): A ticket that authorizes the use of a service within the AD domain. Upon the use of a service, the user requests for a ST to the DC, and uses the ticket to prove its authenticity to the service server.

The flow of the Kerberos authentication upon a users' usage of a service is as follows.

1. User requests a TGT to the DC (KRB_AS_REQ).
2. DC creates a TGT (KRB_AS_REP).
3. User sends the TGT to the DC, and requests for a ST (KRB_TGS_REQ).
4. DC verifies the TGT and if the authenticity of the user is confirmed, provides a ST (KRB_TGS _REP).
5. The user sends the ST to the server that provides the desired service (KRB_AP_REQ).
6. The server verifies the ST, and if confirmed, provides the service.

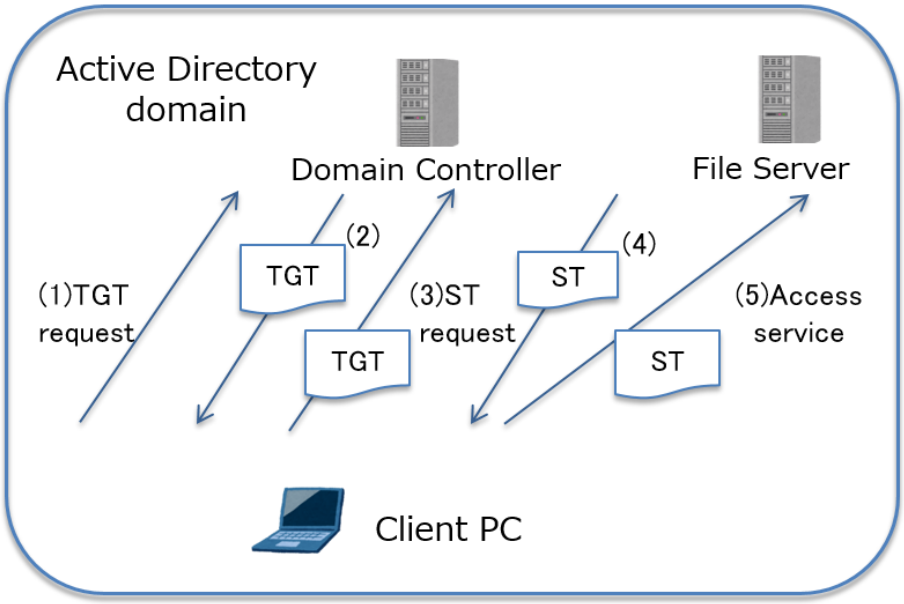

Figure 1. Kerberos authentication

2. Attack against Active Directory

2.1. Steps of attacks against Active Directory

There are several steps of attacks against AD. Attackers who can intrude into an organization network tend to stay inside the network or repeat intrusion multiple times until they are able to accomplish their final goals such as exploiting sensitive information. 2. Attackers firstly steal Domain Users' credential to prepare for get higher privilege. 3. Then try to obtain the Domain Administrator's privileges, which are the highest privileges of an Active Directory environment. MS14-068 and MS17-010 are often used to obtain Domain Administrator's privileges. Attackers who can acquire the Domain Administrator's privileges will likely create a backdoor called the "Golden Ticket" and "Silver Ticket" that disguises itself as a legitimate account in order to obtain long-term administrative privilege.

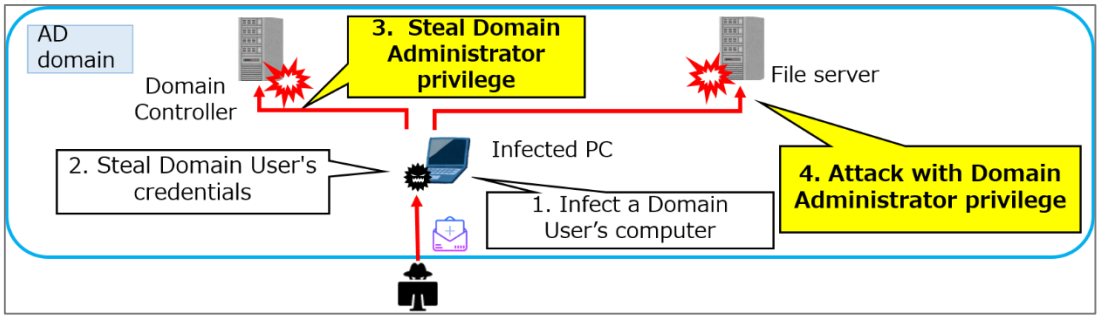

Figure 2. Steps of attacks against AD

This research focuses on attack activities with Administrator privilege (Step 3, 4).

2.2. The Golden Ticket

A Golden Ticket [B] is a TGT created by the attacker that has a legitimate signature. A TGT is signed by the password hash of the krbtgt account that exists on the Domain Controller, and is usually provided by the Domain Controller. However, attackers that have exploited the domain administrative privileges could obtain the password hash of krbtgt, enabling them to create a TGT with legitimate signature for arbitrary accounts. A tool to attack AD environments called mimikatz [C] enables attackers to easily create a TGT with a significantly long term of validity (defaulted to ten years) to any given account in an offline environment. Attackers tend to create a Golden Ticket for the Domain Administrator account. Offline in this context refers to any standalone computer that does not belong to the AD domain, and any environment that cannot communicate with the DC. The extended expiration limit of the Golden Ticket enables the attacker to continuously use it even after the password for the account it disguised is changed. Furthermore, since the Golden Ticket has a legitimate signature, it is difficult to differentiate it from a normal TGT. Since the detection of a Golden

Ticket attack is difficult, these countermeasures are often delayed or never done, leading to increasing numbers of incidents and damages.

2.3. The Silver Ticket

A Silver Ticket [M] is a ST created by the attacker that has a legitimate signature. A ST is signed by the password hash of the corresponding service account exists on the Server, and is usually provided by the Domain Controller. However, attackers that have exploited the administrative privileges of the specific server could obtain the password hash of service account, enabling them to create a ST with legitimate signature for arbitrary accounts. Mimikatz enables attackers to easily create a Silver Ticket with a long term of validity to any given account. Attackers tend to create a Silver Ticket for the specific services such as CIFS [N]. As same as the Golden Ticket, Silver Ticket has a legitimate signature. Moreover, Attackers can use Silver Tickets without accessing the Domain Controller. Thus it is more difficult to detect Silver Ticket attacks.

3. Problems regarding detection of attacks against AD

3.1. Difficulty of detecting attacks against AD

Several methods for detecting attacks against AD have been proposed, for instance comparing process execution logs to a blacklist of tools which attackers tend to use, monitoring authentication requests from unexpected source computers. However, it is difficult to detect attacks in the following reasons.

- **Abuse of legitimate account**: Attackers can leverage legitimate accounts using a Golden Ticket. It is difficult to differentiate these types of attack activities from normal Kerberos authentications.
- **Abuse of built-in windows commands or tools**: Attackers leverage built-in commands or tools in addition to attack tools [D]. Detection is increasingly difficult if attackers change the executable file name of the attack tools.
- **Abuse of legitimate computer**: If attackers are able to compromise the computer which the legitimate administrator uses, detection is more difficult.
- **No trace of attacks on the Domain Controller (Silver Ticket):** Attackers can use Silver Tickets without accessing the Domain Controller.

3.2. Previous research

- **Detection using authentication logs**: Chih-Hung Hsieh et al. use unsupervised machine learning to detect abnormal behavior of users using Event Logs related to authentication [E], focusing on abnormal authentications such as requests from

unexpected computers or accounts. In the research paper, the authors mention that they need improve the recall rate (66%).

- **Detection using process logs:** Michael Gough introduces the signature-based method for detecting processes with blacklists using Event Logs related to processes [F]. However, false negatives can occur if attackers change the file names of the tools since signatures are based on the filename. False positives can occur if legitimate operators use commands which match the signatures for daily operation.
- **Detection through network traffic monitoring**: Several methods are proposed for detecting attacks including the abuse of Golden Ticket and Silver Tickets through monitoring network traffic [G][H][O]. We refer these methods and propose the specific implementation method for reasonable and effective detection.

4. Proposed method

In this research, a real-time detection method for attack activities against Active Directory using Event logs and Kerberos packets is introduced.

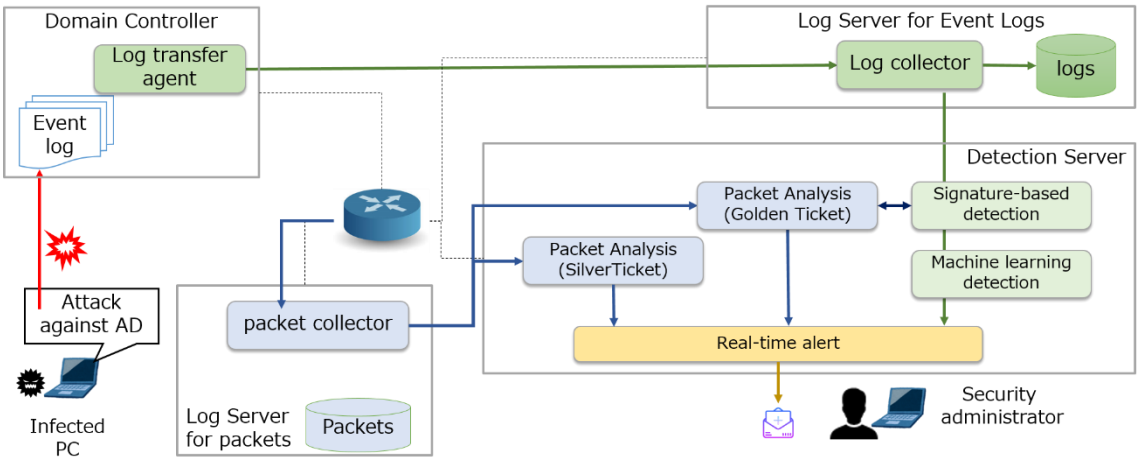

Figure 3. Summary of the proposed method

4.1. Event Log analysis

Event Log analysis consists of the following steps.

1. If someone access to the DC including attacks, activities are recorded in the Event log on DC.
2. Each Event Log is sent to Logstash[i] in real-time by Winlogbeat[ii] (log transfer agent). Logstash extracts input data from the Event log, then call the detection API.

3. Detection API is launched (Detection programs are implemented with Web API). Firstly, analyze the log with signature detection (see 4.1.2. Signature-based detection).
4. If the log matches specific signature (signature B), then analyze the log with machine learning or whitelist (see 4.1.3. Machine learning).
5. If the log matches specific signature (signature D), then analyze the log with packet detection (see 4.2. Packet analysis).
6. If attack is detected, judge the log is recorded by attack activities.
   Send alert E-mail to the security administrator, and add a flag indicates attack to the log (Real-time alert).
7. Transfer the log to Elasticsearch[iii].

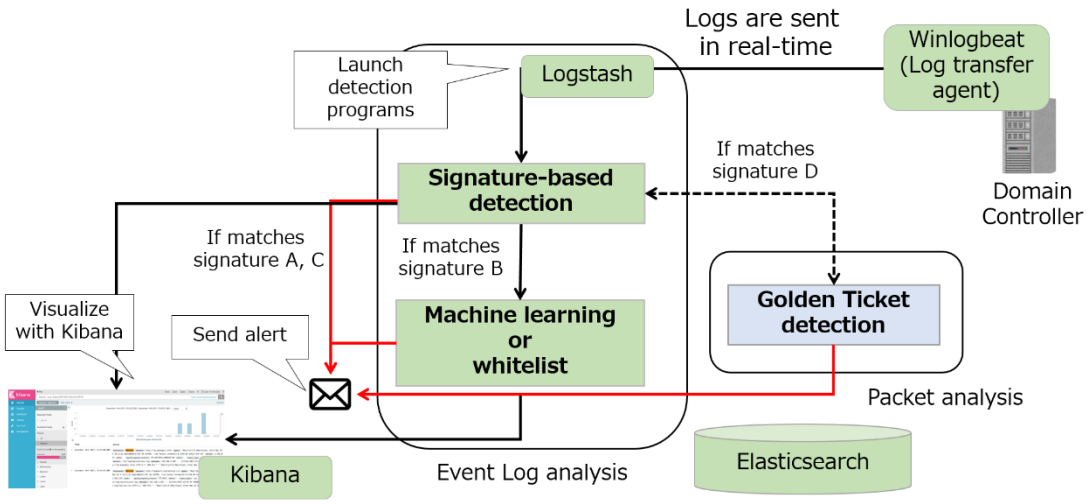

Figure 4. Summary of Event Log analysis

Our method uses two types of detections.

Signature-based detection: Event Logs are first analyzed using several detection signatures based on useful existing methods[A][F][G][H][I] which focus on the characteristics of the attack activities.

Machine Learning or whitelist: Event Logs are analyzed with unsupervised machine learning to detect unusual commands or tools. If attack activities are detected by Signature-based detection, re-analyze with machine learning to reduce false positives. If operational environment is stable, white lists can be used instead of machine learning.

Real-time alert: In order to enable real-time detection, Event Logs are sent to Elastic Stack

in real-time. If attack activities are detected, an alert mail is sent to the security administrator.

4.1.1 Event ID used for detection

The proposed method only uses the Event Logs of the DC for detection. The reasons we focus on the Event Logs of the DC is:

- Attackers tend to access the DC in order to create a Golden Ticket, steal information, and execute other critical tasks.
- DC uniformly handles the authentication of all users and computers, and logs related to authentication are stored in the DC's Event logs.

Our proposed method is practical since it only uses built-in Windows Event Logs and Event Logs of the DC and is relatively easy to implement in a production environment.

We use the event IDs and data shown in Table 2.

Table 2. Event ID used for detection

Event ID	Description	Points for detection	Signature	Machine learning
4672	Special privileges assigned to a new login	Information of accounts that have domain administrative privileges are recorded.	Use	Not Use
4674	An operation was attempted on a privileged object	Logged the process when the specified user exercised the special privileges.	Use	Use
4688	A new process has been created	Logged all processes executed	Use	Use
4768	A Kerberos authentication ticket (TGT) was requested	This event is recorded upon a TGT request. Therefore, when a Golden Ticket is used, this event is not recorded.	Use	Not Use
4769	A Kerberos service ticket was requested	When a service is accessed using a TGT including the Golden Ticket, this event is recorded.	Use	Not Use
5140	A network share object was accessed	This event is recorded when a file sharing service is accessed.	Use	Not Use

We use the data columns shown in Table 3 and Table 4.

Table 3. Data column in each Event ID used for detection (Signature-based detection)

Column Name	4672	4674	4688	4768	4769	5140
Account Name	Use	Use	Use	Use	Use	Use
Client Address	-	*	*	Use	Use	Use
Process Name	-	Use	Use	-	-	-
Object Name	-	Use	-	-	-	-
Service Name	-	-	-	Use	Use	-
Shared Name	-	-	-	-	-	Use

*: Event ID 4674 and 4688 have no information of source IP address. The proposed method identifies source IP address information from Event ID 4769 recorded just before Event 4674/4688 for each accounts. Because there is a high possibility that Service Ticket is requested before command/tools execution.

Table 4. Data column in each Event ID used for detection (machine learning)

Column Name	4672	4674	4688	4768	4769	5140
Account Name	Not use	Use	Use	Not use	Not use	Not use
Client Address		-	-			
Process Name		Use	Use			
Object Name		Use	-			
Service Name		-	-			
Shared Name		-	-			

In Event ID: 4688, information of all executed processes including those of normal privileged users. On the other hands, in Event ID: 4674, specific processes executed with special privileges are recorded. The reason why we use both Event ID: 4674 and 4688 for detection is as follows.

- Information of temporary exe files (%SystemRoot%PSEXESVC.exe) created on the destination computer when it is accessed remotely by Psexec[iv] is recorded in Event ID:4674. The information is useful for the detection of Psexec since the temporary file name is constant even if attackers changed the file name of the tool.

- It is specific condition that executed commands are recorded in Event ID: 4674. For instance, when commands are executed on the remote computer by using Psexec or wmic with loaded credentials on a source computer's memory. Attackers tend to

load the credentials in the same way to use the Golden Ticket and access to the target computer remotely.

4.1.2. Signature-based detection

In order to minimize false negative rate, “Signature-based detection” uses multiple signatures focusing on characteristics of attacks against AD especially with the Golden Ticket attacks. It detects a log as positive if a log matches any single signature. If there is a list of Domain Administrator accounts used for operations, the list (admin list) is useful for detection.

Signatures for Signature-based detection:

A) Unexpected administrative privilege use
B) Execution of tools attackers tend to use
C) Use of administrative shared resource
D) ST requests without a prior TGT request.
E) Attack leveraging MS17-010 is detected

The specific detail of the detection algorithm is shown in Figure 5.

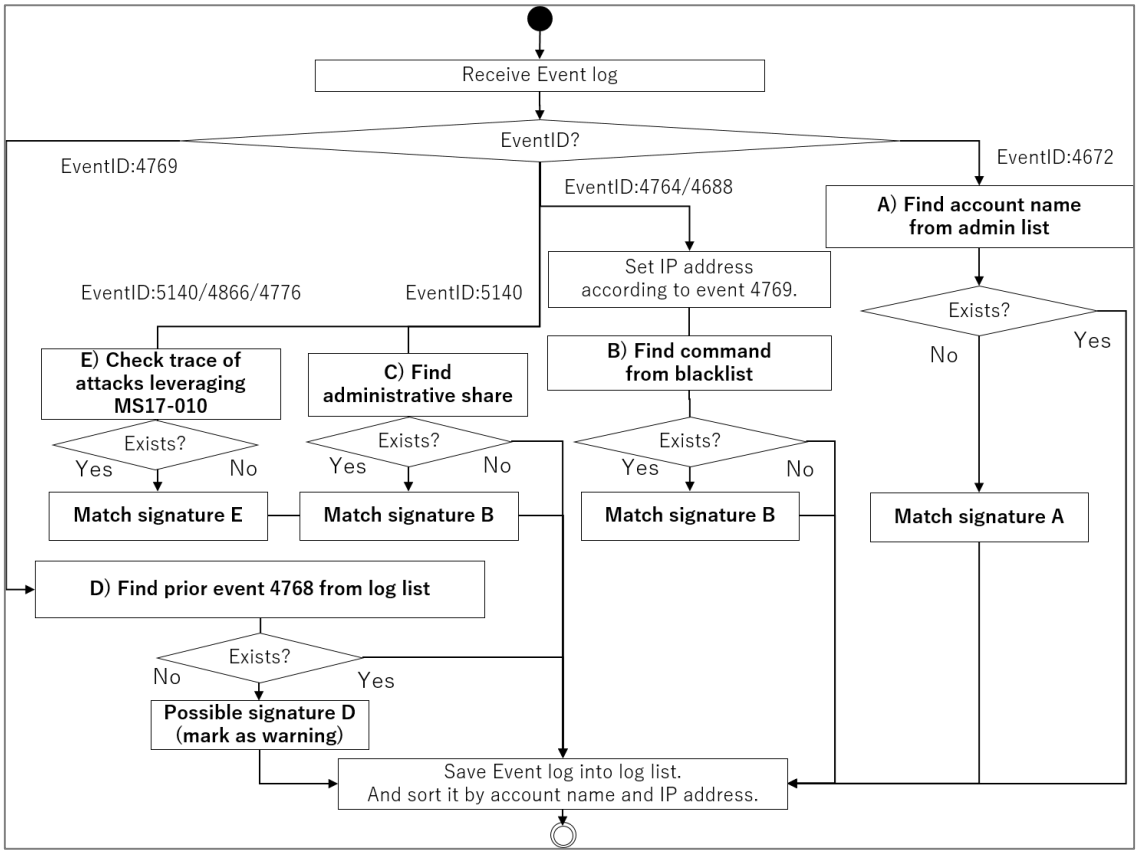

Figure 5. The algorithm of Signature-based detection

If a log matches any single signature A or C, there is a high possibility of attack. Then judge the log was recorded by attack activity and raise an alert.

Each detection signature is show in Table 5-8.

Table 5. Detection signatures (A)

A) Unexpected administrative privilege use	
Summary	Monitor privilege use which are not expected to be used in operations.
Useful for	Detecting privilege escalation such as the use of vulnerability MS14-068 (CVE-2014-6324)
Detection method	Compare accounts recorded in Event ID:4672 with an administrator account list in the operational environment.

Table 6. Detection signatures (B)

B) Execution of tools attackers tend to use	
Summary	Monitor execution of tools attackers tend to use.
Useful for	Detecting attack activities such as remote access or task creation
Detection method	Register CLI tools which are tend to be used for attacks in the blacklist. In our method, the commands shown in [D] are registered in the blacklist. Compare process information recorded in Event ID:4674 and 4688 with commands in the black list. For pre-process, add IP address information to Event ID 4674 and 4688 Extract IP address information from Event ID 4769 (service ticket request) recorded just before Event ID 4674, 4688.

Table 7. Detection signatures (C)

C) Use of administrative shared resource	
Summary	Monitor use of administrative shared resource*.
Useful for	Detecting activities such as placing attack tools or stealing information using administrative shared resource
Detection method	Extract administrative shared resources such as “¥c$” recorded in Event ID:5140.

* Hidden network shares of Windows NT family that allow administrators to have remote access to every disk volume remotely.

Table 8. Detection signatures (D)

D) ST requests without a prior TGT request	
Summary	Monitor ST requests without a prior TGT request.
Useful for	Detecting use of the Golden Ticket (When attacker use Golden Ticket, TGT request events are not recorded before ST request.)
Detection method	Extract Event ID:4768(TGT request) and 4679(ST request), and sort by account and computer. Then find Event ID 4769 without corresponding 4768.
Remarks	ST request occur without a prior TGT request under limited conditions because of the Kerberos specification. Thus if a log matches signature D, our method marks the log as “warning”. Then it compares with the detection result of packer analysis (see 4.2. Packet analysis).

Table 9. Detection signatures (E)

E) Attack leveraging MS17-010 is detected	
Summary	Attack leveraging the vulnerability fixed in MS17-010 is detected.
Useful for	Detecting attacks leveraging MS17-010
Detection method	Windows 2016: Extract Event ID:5140 then check whether all logs are recorded within 2 seconds which match the following conditions. - Shared Name is “IPC$” and Account Name ends with “$” (computer account) - Shared Name is “C$” “admin$” (administrative share) and Account Name ends with “$” (computer account) Windows 2012 / Windows 8 Check whether all logs are recorded twice from the same IP address and account within few seconds which match the following conditions. - Event ID 5140: Shared Name is “IPC$” - Event ID 4624 - Event ID 4776 Windows 2008 R2 / Windows 7

	Extract Event ID:5140, 4688 then check whether all logs are recorded within 2 seconds which match the following conditions. - Security ID is “SYSTEM” and Process Name contains “cmd.exe” - Security ID is “ANONYMOUS LOGON” and Shared Name is “IPC$”
Remarks	Since attack methods are different among the target Windows version , our method use unique signature for each Windows version.

4.1.3. Machine learning

For signature B (Execution of tools attackers tend to use) of signature-based detection, a lot of false positive can be occurred depending on daily operations (e.g. A Domain Administrator often use some commands in the blacklist) since it detects a log as positive if a log matches any single command in the blacklist. On the other hand, “Machine Learning” can reduce false positives through re-analyzing the detected commands with machine leaning. Machine Learning can detect anomaly commands comparing with logs of the normal state, so administrators can easily find out whether the result is true positive (attack) or false positive.

Machine Learning gives computer systems the ability to "learn" with data without being explicitly programmed and recognizes pattern. It's divided into supervised and unsupervised learning. Supervised learning requires that the outputs are already known and that the data used for training should be labeled with correct answers. On the other hand, unsupervised learning does not require labels of correct answers.

We use unsupervised learning, because it is difficult to label the correct answers for attack detection, since it is difficult to differentiate logs recorded by attacks.

The method analyzes Event Logs related to process (Event ID: 4674, 4688) which match signature B (Execution of tools attackers tend to use).

If the operational environment is stable, whitelists can be used instead of machine learning. The name of commands or tools used in daily operation should be specified in the whitelist as shown in Figure 6.

```
"processname"
"c:¥windows¥system32¥ipconfig.exe"
"c:¥windows¥system32¥ping.exe"
```

Figure 6. White list example

4.2. Packet analysis

Packet analysis helps to improve The detection rate for Golden Ticket detection and provide a method to detect Silver Ticket attacks. In 4.1. Event Log analysis, we introduce signature D for Golden Ticket detection, however sometimes false positive occurs because of the Kerberos specification. It is possible to detect attacks with higher detection rate by using packet analysis in addition to Event Log analysis.

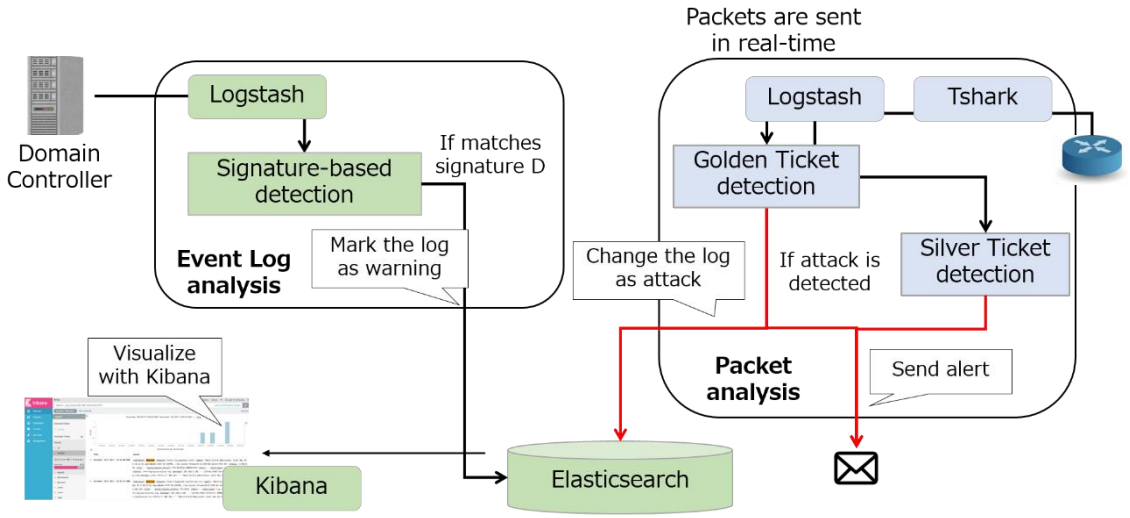

Figure 7. Summary of packet analysis

4.2.1 Packets used for detection

Table 10 shows the Kerberos message type used for detection.

Table 10. Packets used for detection

Message type	Message type name	Description
11	KRB_AS_REP	A response from DC for AS exchange. KRB_AS_REP contains a ticket (TGT) for the client.
12	KRB_TGS_REQ	A request for DC for Ticket-Granting Service (TGS) Exchange. KRB_TGS_REQ should contain the same ticket provided in KRB_AS_REP or KRB_TGS_REP.

13	KRB_TGS_REP	A response from DC for Ticket-Granting Service (TGS) Exchange. KRB_TGS_REP contains a ticket for the requested server or for a ticket granting server.
14	KRB_AP_REQ	A request for the server for client/server authentication (CS) exchange. KRB_AP_REQ should contain the same ticket provided in KRB_TGS_REP.
32	KRB_AP_ERR_TKT_EXPIRED	An error response for KRB_AS_REP. If the current time is later than end time of the ticket, the KRB_AP_ERR_TKT_EXPIRED error is returned.

Figure 8 shows the algorithm of packet analysis.

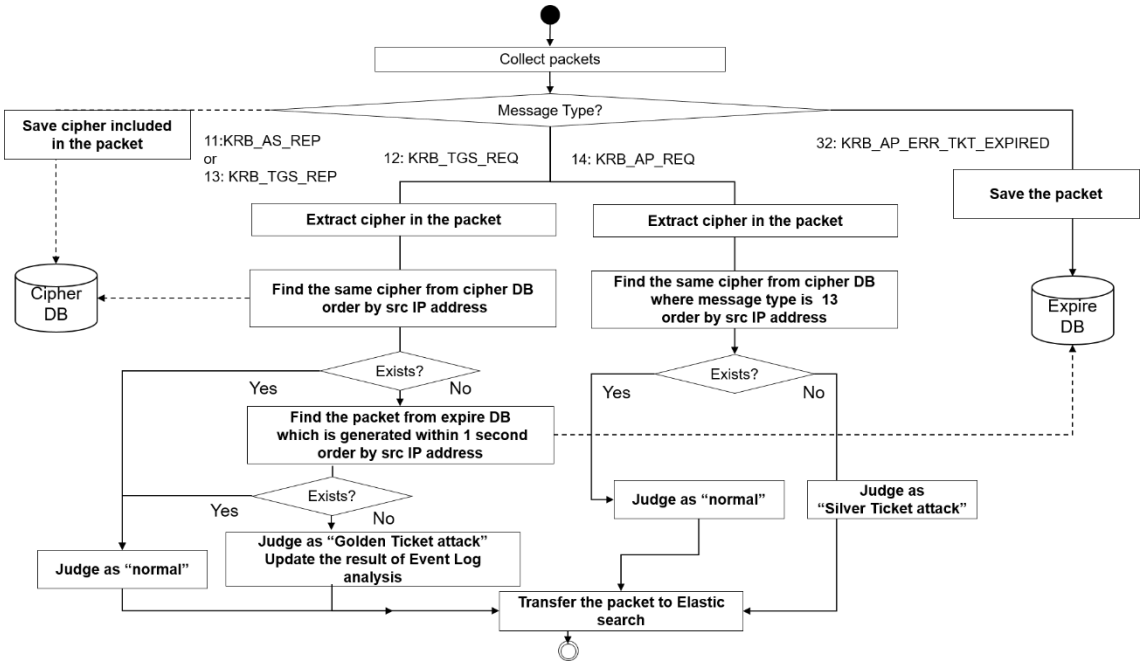

Figure 8. Algorithm of packet analysis

4.2.2 Golden Ticket detection

Normally, KRB_TGS_REQ contains the same ticket provided in KRB_AS_REP or KRB_TGS_REP. On the other hands, since Golden Ticket is the TGT which attackers create, thus when attacker use Golden Ticket, KRB_TGS_REQ is generated without corresponding KRB_AS_REP. This activity can be detected by signature D (see 4.1. Event Log analysis), however we found that sometimes this behavior occurs in normal operations because of

the Kerberos specification[P] and it causes false positives. Therefore, “packet analysis” analyzes logs which are marked as “warning” by Event Log analysis.

- **How to find the Golden Ticket included in KRB_TGS_REQ**

1. Extract encrypted tickets (cipher value) from KRB_AS_REP packets show in Figure 9.

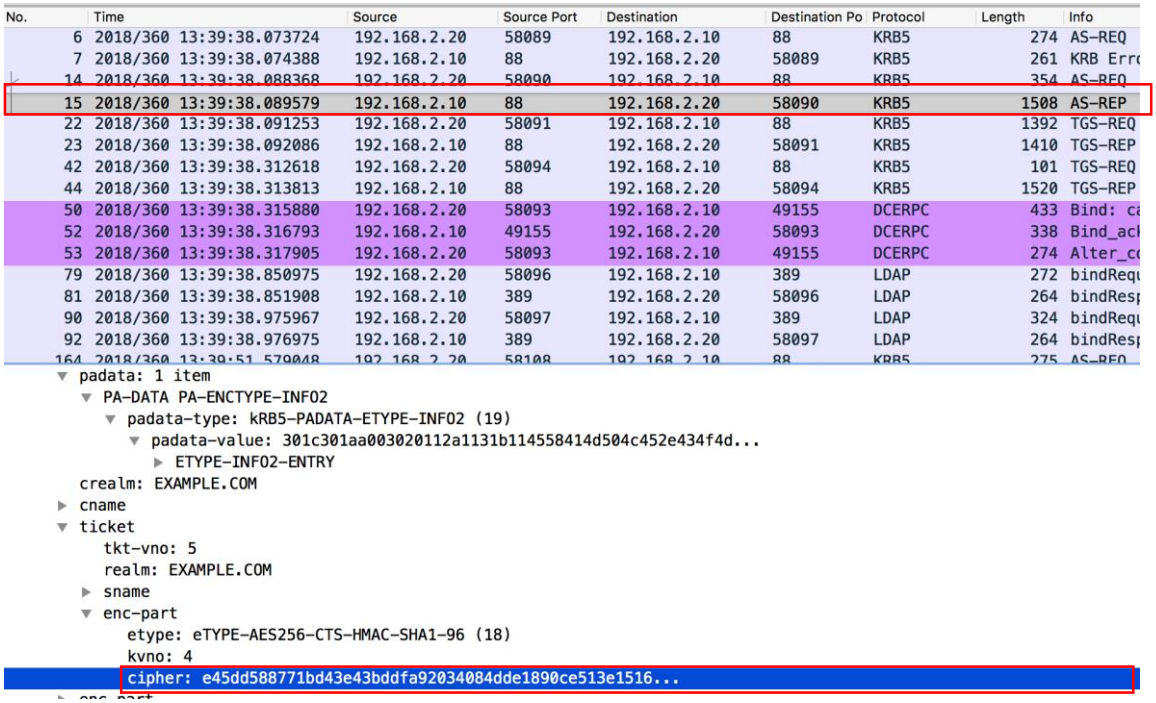

Figure 9. Kerberos packet of KRB_AS_REP

Then extract cipher value from KRB_TGS_REP packets in the same way.
Extracted KRB_AS_REP and KRB_TGS_REP packets are stored in database during 10 hours since the default expiration period of Kerberos tickets is 10 hours.

2. Extract encrypted tickets (cipher value) from KRB_TGS_REQ packets show in Figure 10.

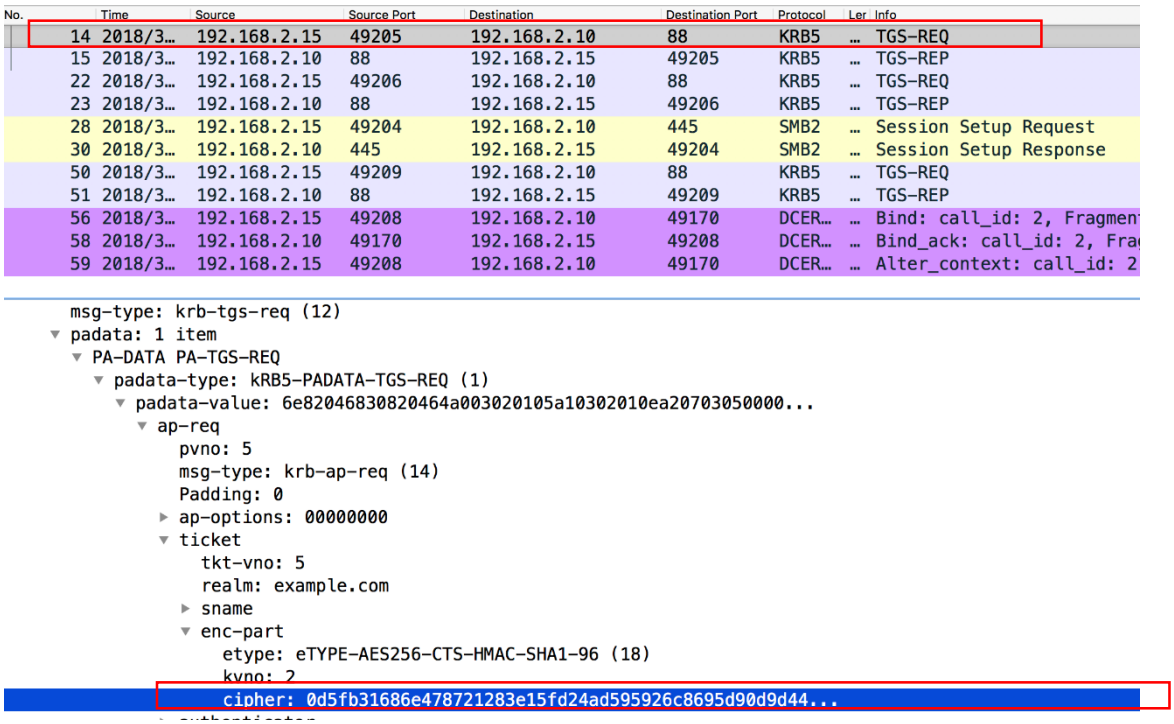

Figure 10. Kerberos packet of KRB_TGS_REQ

If KRB_TGS _REQ contains new a cipher which is not generated by the past KRB_AS_REP or KRB_TGS_REP, Golden Ticket attack is suspected.

- **How reduce false positives**

Even if a ticket has expired, the client sends the request which contains the expired ticket by design of the Windows. This causes false positives. Thus if new cipher is found in KRB_TGS _REQ, our method checks whether KRB_AP_ERR_TKT_EXPIRED packet will be generated within 1 seconds from the same source IP address. If so, our method judge the packet is generated by normal operations.

4.2.3 Silver Ticket detection

Normally, KRB_AP_REQ contains the same ticket provided in KRB_TGS_REP. On the other hands, since Silver Ticket is the ST which attackers create, thus when attacker use Silver Ticket, KRB_AP _REQ (see Figure 11) contains new a ticket which is not generated by the past KRB_TGS_REP.

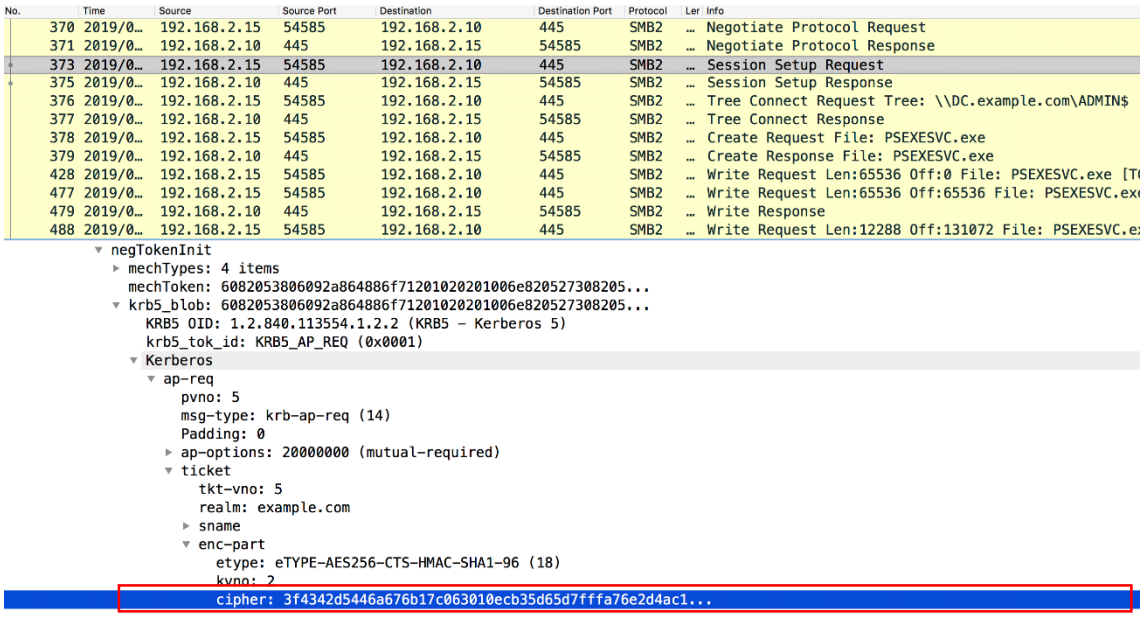

Figure 11. Kerberos packet of KRB_AP_REQ

4.3. Identification of tactics in ATT&CK

ATT&CK is a knowledge base of adversary tactics and techniques [Q]. It is getting common recently. We also introduce the method to identify the possible tactics for each detected attack activity automatically.

Table 11 shows our method support for identification of tactics defined in ATT&CK.

Table 11. Tactics defined in ATT&CK

ID	Tactics name	Description	Our method support
TA0001	Initial Access	The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network.	×
TA0002	Execution	The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.	○ Signature B
TA0003	Persistence	Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.	○ Signature B Signature D Golden Ticket Silver Ticket

TA0004	Privilege Escalation	Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network.	○ Signature A
TA0005	Defense Evasion	Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses.	○ Signature B
TA0006	Credential Access	Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment.	×
TA0007	Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network.	○ Signature B
TA0008	Lateral Movement	Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could.	○ Signature B Signature C
TA0009	Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration.	○ Signature B Signature C
TA0010	Exfiltration	Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network.	×
TA0011	Command and Control	The command and control tactic represents how adversaries communicate with systems under their control within a target network.	×

t	computer_name	dc2016.example2.local
t	event_data.MandatoryLabel	S-1-16-12288
t	event_data.NewProcessId	0x8d8
t	event_data.NewProcessName	C:\Windows\System32\at.exe
t	event_data.ParentProcessName	C:\Windows\System32\cmd.exe
t	event_data.ProcessId	0x49c
t	event_data.SubjectDomainName	EXAMPLE2
t	event_data.SubjectLogonId	0x3d26b
t	event_data.SubjectUserName	administrator
t	event_data.SubjectUserSid	S-1-5-21-388095587-3916525220-2479421359-500
t	event_data.TargetDomainName	-
t	event_data.TargetLogonId	0x0
t	event_data.TargetUserName	-
t	event_data.TargetUserSid	S-1-0-0
t	event_data.TokenElevationType	%%1936
#	event_id	4,688
t	host.name	dc2016
t	indicator	attack: command on blackList is used
t	keywords	Audit Success
t	level	Information
t	log_name	Security
t	message	A new process has been created.\u000d\u000a\u000d\u000aCr ccount Name:\u0009\u0009administrator\u000d\u000a\u0009Ac u000d\u000a\u0009Security ID:\u0009\u0009S-1-0-0\u000d\u0 90x0\u000d\u000a\u000d\u000aProcess Information:\u000d\u0 a\u0009Token Elevation Type:\u0009%%1936\u000d\u000a\u000 ess Name:\u0009C:\Windows\System32\cmd.exe\u000d\u000a\u0 d to the new process in accordance with User Account Cont is only used if User Account Control is disabled or if th ith no privileges removed or groups disabled. An elevate or. An elevated token is also used when an application i r of the Administrators group.\u000d\u000a\u000d\u000aTyp used when User Account Control is enabled, the applicatio or.
t	opcode	Info
#	process_id	4
t	provider_guid	{54849625-5478-4994-A5BA-3E3B0328C30D}
t	record_number	204882
t	source_name	Microsoft-Windows-Security-Auditing
?	tactics	⚠ TA0003

Figure 12. Kerberos packet of KRB_AP_REQ

5. Evaluation of proposed method

5.1. Evaluation method

We evaluate whether attacks against Active Directory can be correctly detected using the proposed method. The Evaluation environment is shown in Table 12.

Table 12. Evaluation environment

	OS	Number of computers
DC	Windows Server 2016	1
File server	Windows Server 2008 R2	1
Client Computer	Windows 7 (x64)	38

We conduct mock APT attack against the AD assuming that a legitimate Domain Administrator's account and a legitimate administrator account of file server is leveraged (Table 13).

Table 13. Contents of attack

No	Leveraged account	Attack activities
1	Domain user (User101)	Take over the Domain Administrator privilege using a privilege escalation vulnerability (**MS14-068**).
2	SYSTEM	Take over the Administrator privilege using a vulnerability (**MS17-010**).
3	Domain user (User101 with Domain Administrator privilege)	Mount C drive of DC using **administrative share** by **net command**.
4	Domain user (User101 with Domain Administrator privilege)	Create **Golden Ticket for a legitimate Domain Administrator** (administrator).
5	Domain Administrator (administrator)	Remote access to DC with **PsExec** and execute commands using Golden Ticket.
6	Administrator account of file server (fsadmin)	Create **Silver Ticket for a legitimate administrator account of file server** (fsadmin).
7	Administrator account of file server (fsadmin)	Remote access to file server with **PsExec** and execute commands using Silver Ticket.

Commands and tools used during the attack is shown in Table 14. There is a possibility that attackers use other commands, however we use the least commands in order to accomplish the attack.

Table 14. Commands and tools used during the attack

Type	Commands and tools used during the attack

Attack tool	mimikatz
Tool provided by Microsoft	psexec
Built-in Windows command	klist
Built-in Windows command	ipconfig
Built-in Windows command	ping
Built-in Windows command	hostname
Built-in Windows command	net
Built-in Windows command	copy
Built-in Windows command	at

5.2. Evaluation Result of the proposed method

The detection result of the proposed method in shown in Table 15. Table 15 shows whether our method can detect each attack shown Table 13.

Table 15. Detection result of the proposed method

Attack No	Detection result
1	○
2	○
3	○
4	○
5	○
6	○
7	○

○：Can detect the attack

×：Cannot detect the attack

As a result, our proposed method yielded high recall rate. Also we were able to reduce false positives and improve the precision by using packet analysis.

5.3. Remarks on the Evaluation result

- A False negative detection occurs if all the following conditions are satisfied.
  - Attackers use the same commands that legitimate domain administrators use in their daily operations
  - Attackers compromise legitimate domain administrator accounts and their computer
  - Attackers use windows commands which are not in the blacklist

- False positive detection can occur if legitimated Domain Administrators use the commands which in not frequently used in the daily operation. False positive rate depends on environment (e.g. learning period, commands etc.). However, it is possible to find out whether the result is false positive or not through checking detection result periodically.

- Duration of gathering Windows Event Logs for machine learning detection (learning period) depends on environment and operations. In our environment, we required the Windows Event Logs for about one week to achieve sufficient recall and precision.

- Detection using Event ID 4674 achieved higher detection rate, but recorded commands or tools in Event ID 4674 were limited. It records only "ipconfig", "hostname", "netstat" and "psexec" as far as our Evaluation. Therefore, if attackers use other commands for attacking, false negative is occurred using only Event ID 4674.On the other hand, Event ID 4688 records more commands than Event ID 4674. We suggest using not only Event ID 4674 but also Event ID 4688 for detection in order to reduce false negative.

6. Consideration for implementation

The followings are recommendations aspects of operation in order to detect attacks effectively using the proposed method.

- Minimize the number of accounts who have Domain Administrator's privilege, and the computers they use for access the Domain Controller.

- Enter ID and password of the Domain Administrator account explicitly every time when you access the Domain Controller from client computers remotely. Do not login to client computers with Domain Administrator accounts as much as possible. In case of Single Sign-On login (a login method using loaded credentials on memory of the source computer), trace of access is recorded in Event ID:4674 as same as attackers' access using malicious authentication ticket such as Golden Ticket. If Single Sign-On login is used in daily operations, it is difficult to detect attacks as anomalies. On the other hand, if you access with ID /password every time, it is easy to detect attacks since Event ID:4674 is rarely recorded in the clean environment.

- Save the evidences of maintenance operations with Domain Administrator's privilege (e.g. date, account, computer, operations). These evidences help administrators to judge whether detected operations are false positive or not.

7. Summary

The abuse of a Domain Administrator means the AD is under the full control of the attacker, and thus requires immediate action. However, detecting attacks is difficult if legitimate administrator accounts are abused such as Golden Ticket / Silver Ticket attacks

In this research, we propose an implementation method for detecting attacks with combination of Event Log analysis and packet analysis. Our detection method can detect attacks in timely manner, and yields a high detection rate even if legitimate accounts or built-in commands are leveraged. Moreover, our method can detect Silver Ticket attacks which was said to be difficult to detect.

The proposed method is practical since it uses only built-in Windows Event Logs of Domain Controller and minimum Kerberos packets, so it is relatively easy to implement in running environments.

Reference

[A] Shingo Abe, Detecting Lateral Movement in APTs, https://www.first.org/resources/papers/conf2016/FIRST-2016-105.pdf

[B] Skip Duckwall, Benjamin Delpy, Abusing Kerberos, https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf

[C] mimikatz, https://github.com/gentilkiwi/mimikatz/releases

[D] JPCERT Coordination Center, Windows Commands Abused by Attackers, http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

[E] Chih-Hung Hsieh, AD2: Anomaly Detection on Active Directory Log Data for Insider Threat Monitoring, Institute of Information Industry Taipei

[F] Michael Gough, "Finding Advanced A*acks and Malware With Only 6 Windows EventID's," Splunk Inc

[G] Idan Plotnik, "System, method and process for detecting advanced and APT attacks with the recoupling of Kerberos authentication and authorization,"

[H] Darren B Schwartz, "Systems and methods for detecting and reacting to malicious activity in computer networks,"

[I] Junghoon Oh, "A Forensic Analysis of APT Lateral Movement in Windows Environment," AhnLab

[J] One-class SVM with non-linear kernel (RBF), http://scikit-learn.org/stable/auto_examples/svm/plot_oneclass.html

[K] IsolationForest example, http://scikit-learn.org/stable/auto_examples/ensemble/plot_isolation_forest.html#sphx-glr-auto-examples-ensemble-plot-isolation-forest-py

[L] Anomaly detection with Local Anomaly Factor (LOF), http://scikit-learn.org/stable/auto_examples/neighbors/plot_lof.html#sphx-glr-auto-examples-neighbors-plot-lof-py

[M] How Attackers Use Kerberos Silver Tickets to Exploit Systems, https://adsecurity.org/?p=2011

[N] [MS-CIFS]: Common Internet File System (CIFS) Protocol , https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/d416ff7c-c536-406e-a951-4f04b2fd1d2b

[O] Detecting and reacting to malicious activity in decrypted application data, US10057282B2, https://patents.google.com/patent/US10057282B2/en

[P] The Kerberos Network Authentication Service (V5), https://tools.ietf.org/html/rfc4120

[Q] ATT&CK, https://attack.mitre.org/

---

[i] An open source data processing pipeline that ingests data from a multitude of sources provided by elastic.

[ii] An open source log transfer agent for Windows Event log provided by elastic.

[iii] An open source data search and analytics engine provided by elastic.

[iv] Remote access CLI tool provided by Microsoft.