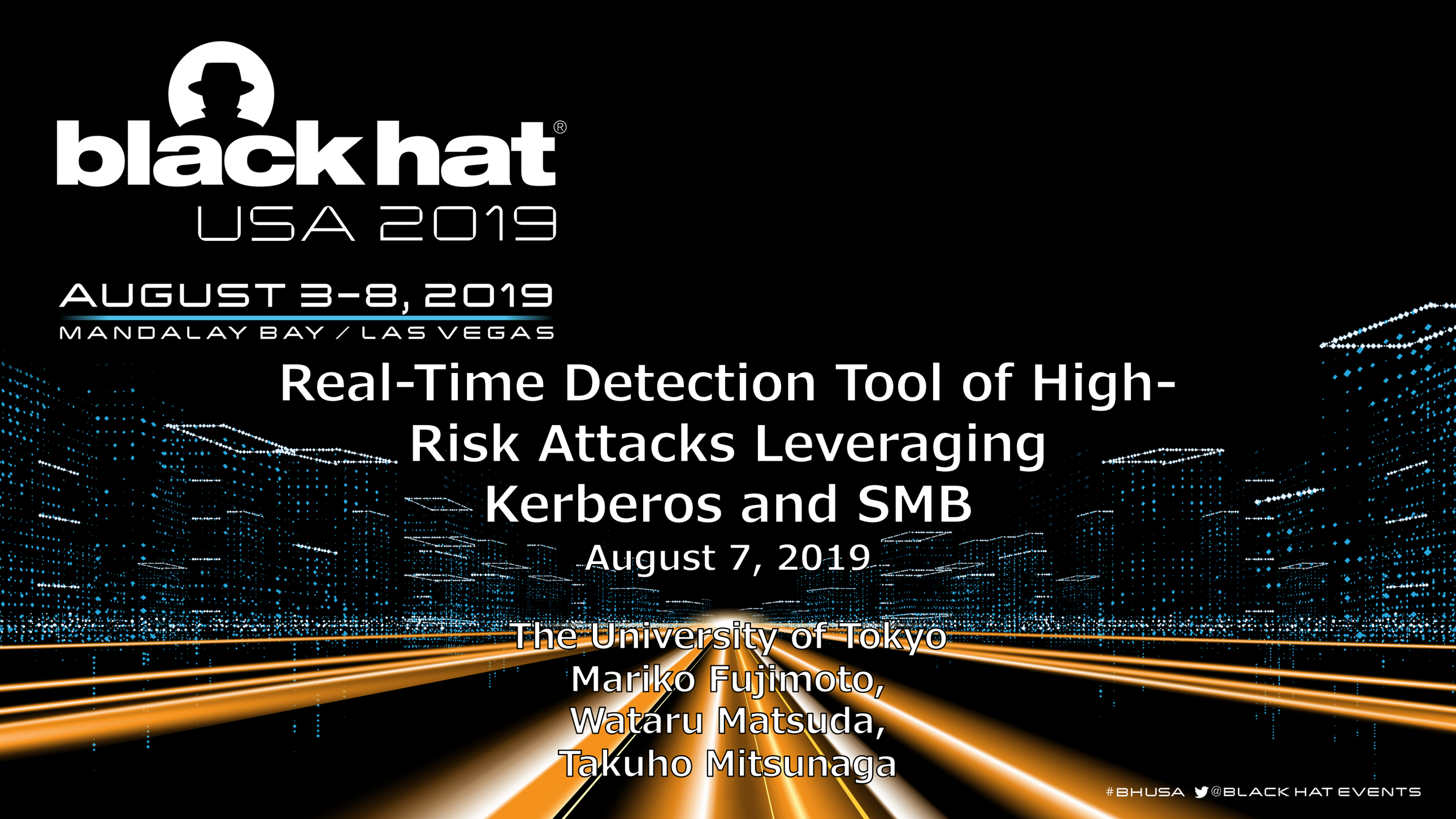


Real-Time Detection Tool of High-Risk Attacks Leveraging Kerberos and SMB

August 7, 2019

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

Introduction

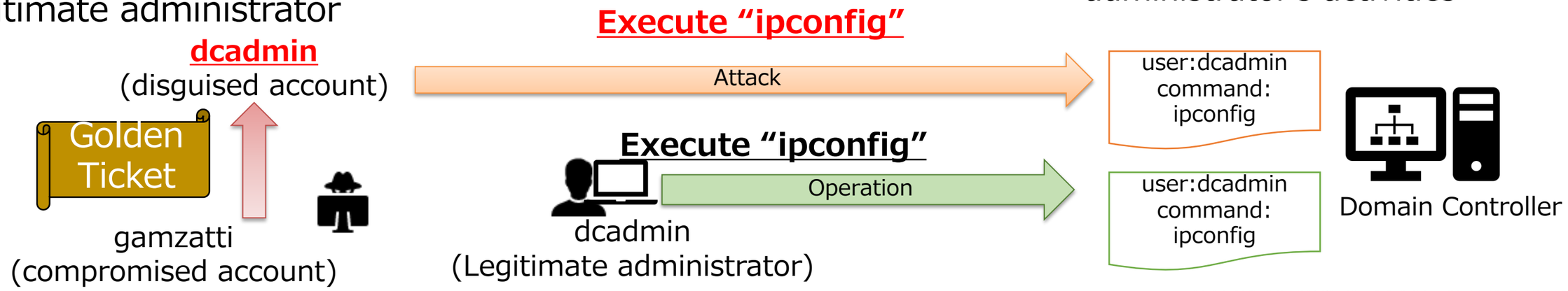
- In targeted attacks, attackers tend to attack Active Directory (AD) in order to expand infections
- Attackers try to take over **Domain Administrator privileges** and create backdoors called the "**Golden Ticket**" and "**Silver Ticket**"
- Attackers leverage the Golden / Silver Ticket to disguise themselves as **legitimate administrator accounts** to avoid detection **for a long period**
- We've implemented a real-time detection tool utilizing **Domain Controller Event Logs** and **Packet Data** to detect attack activities against AD

Difficulty in detecting the Golden Ticket

- The Golden Ticket is a **ticket-granting ticket (TGT)** created by the attackers with a **legitimate signature** and **a long term of validity** (e.g., ten years)
- Attackers can disguise themselves as **arbitrary legitimate administrator accounts** for a long period
- Identifying the use of the Golden Ticket from Event Logs is challenging because **logs are recorded as legitimate administrator's activities**

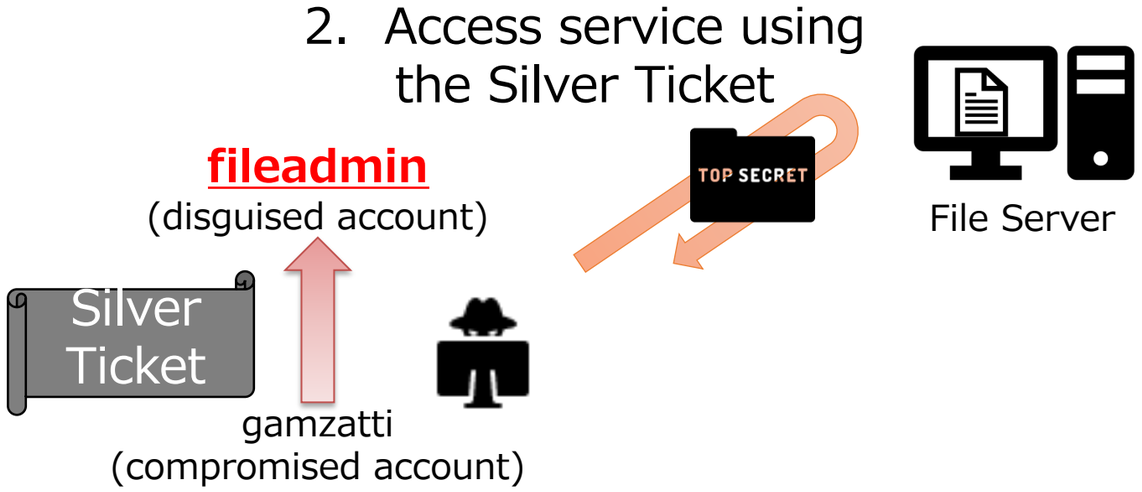
1. Attacker disguises him as legitimate administrator

2. Logs are recorded as legitimate administrator's activities



Difficulty in detecting the Silver Ticket

- The Silver Ticket is a **Service ticket** created by the attackers with a **legitimate signature** and **a long term of validity**
- Attackers can use **specific Windows service** (e.g., file sharing, remote access, etc.) as **arbitrary legitimate accounts** for a long period
- Detecting Silver Ticket is more difficult than Golden Ticket since **no attack trace is left on the Domain Controller**



No trace is left on the Domain Controller

Summary of our detection tools

- We have implemented a real-time detection for typical attack activities against AD
- Our tools use **Event Logs and packet data** (Kerberos & SMB)
- We can detect typical attacks using Event Logs to a certain degree, but packet data helps the accurate detections
- Our tools can identify **ATT&CK** tactics of each detected event

Methods	Overview	Detectable attack activity
Detection with Event Logs	Analyze Event Logs on Domain Controller	• EternalBlue attack (exploit against vulnerability fixed in MS17-010) • Privilege escalation • Suspicious commands • Administrative sharing
Detection with packet data	Analyze Kerberos and SMB packet data among AD domain	• Golden Ticket use • Silver Ticket use

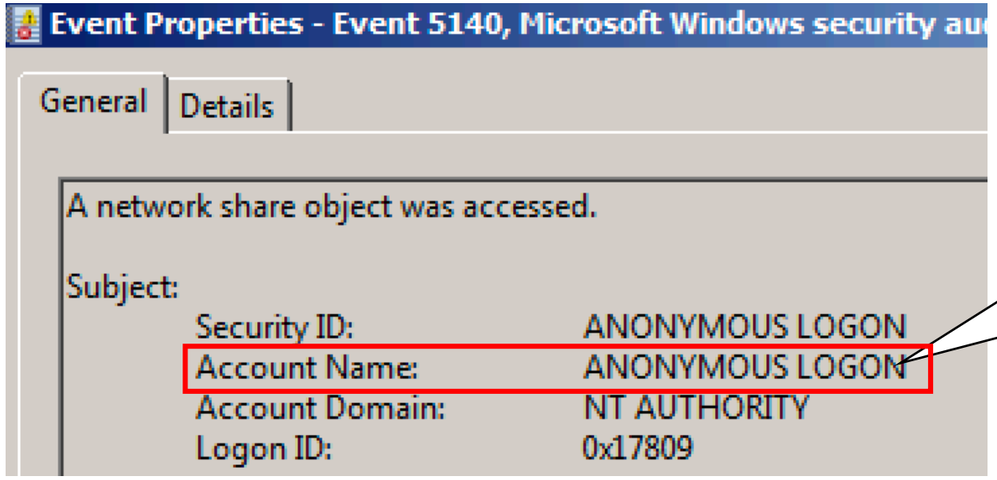
ATT&CK

ATT&CK™

- ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations defined by MITRE
- ATT&CK organizes the flow of cyber attacks using Tactics, Techniques and Procedures
- **Tactics indicates attackers' purpose**
- Examples of tactics:
  - TA0002: Execution (The adversary is trying to run malicious code.)
  - TA0003: Persistence (The adversary is trying to maintain their foothold.)
  - TA0008: Lateral Movement (The adversary is trying to move through your environment.)

Example of detection using Event Logs

- Our tools monitors suspicious activities **leveraging Domain Administrator privilege**
- One of methods to take over the Domain Administrator privilege is leveraging the vulnerabilities fixed in MS17-010 (EternalBlue attack)
- Our tool monitors several characteristics of events in chronological order by attacks
- The following is an example of characteristics event

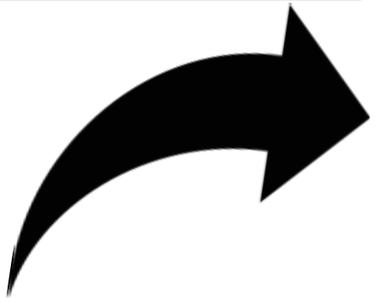


ANONYMOUS LOGON on Event ID: 5140

Detection using packet data

- Our tools detect the Golden / Silver Tickets using Kerberos and SMB packet data among AD domain
- We focus on **Kerberos cipher** in the packet data
- Kerberos cipher is an **encrypted Kerberos ticket** (including the Golden / Silver Tickets) that has a unique random value

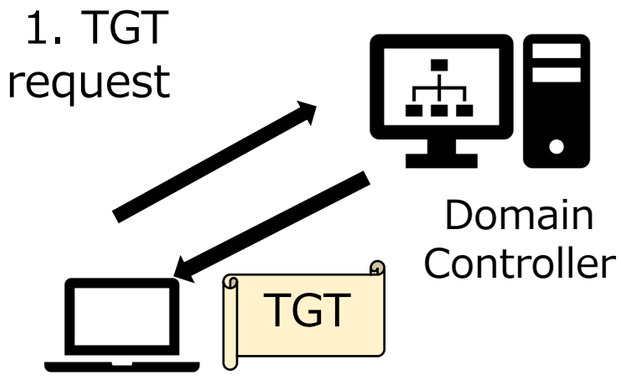
```
    40 2018-12-08 13:58:29.321052   192.168.2.15          192.168.2.10          KRB5          1488 TGS-REQ
    41 2018-12-08 13:58:29.322162   192.168.2.10          192.168.2.15          KRB5          1408 TGS-REP
    48 2018-12-08 13:58:29.323503   192.168.2.15          192.168.2.10          KRB5          1322 TGS-REQ
    49 2018-12-08 13:58:29.324245   192.168.2.10          192.168.2.15          KRB5          1260 TGS-REP
▶ Frame 41: 1408 bytes on wire (11264 bits), 1408 bytes captured (11264 bits) on interface 0
▶ Ethernet II, Src: Vmware_9e:78:37 (00:0c:29:9e:78:37), Dst: Apple_96:d3:a8 (78:4f:43:96:d3:a8)
▶ Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2.15
▶ Transmission Control Protocol, Src Port: 88, Dst Port: 54342, Seq: 1, Ack: 1435, Len: 1354
▼ Kerberos
  ▶ Record Mark: 1350 bytes
  ▼ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: example.com
    ▶ cname
    ▼ ticket
        tkt-vno: 5
        realm: EXAMPLE.COM
      ▶ sname
      ▼ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 11
          cipher: 0a589e1299aa5f6f0d327d25957fab46028139aa8ef71bd5...
    ▶ enc-part
```

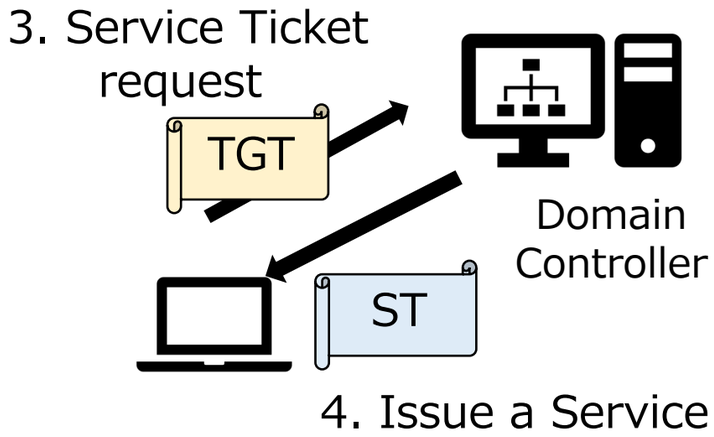


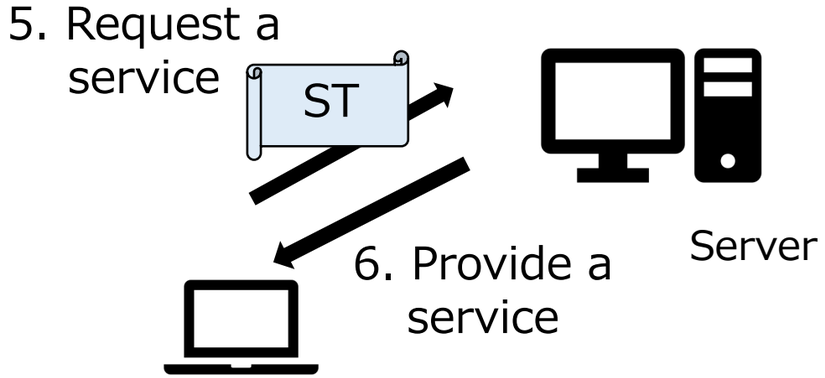
Encrypted Kerberos ticket

Normal user authentication process

1. A user sends TGT requests to Domain Controller
2. **Domain Controller issues a TGT**
3. The user requests Service Ticket to Domain Controller **with TGT**
4. **Domain Controller issues a Service Ticket**
5. The user requests the server to use a service **with Service Ticket**
6. The server provides the corresponding service

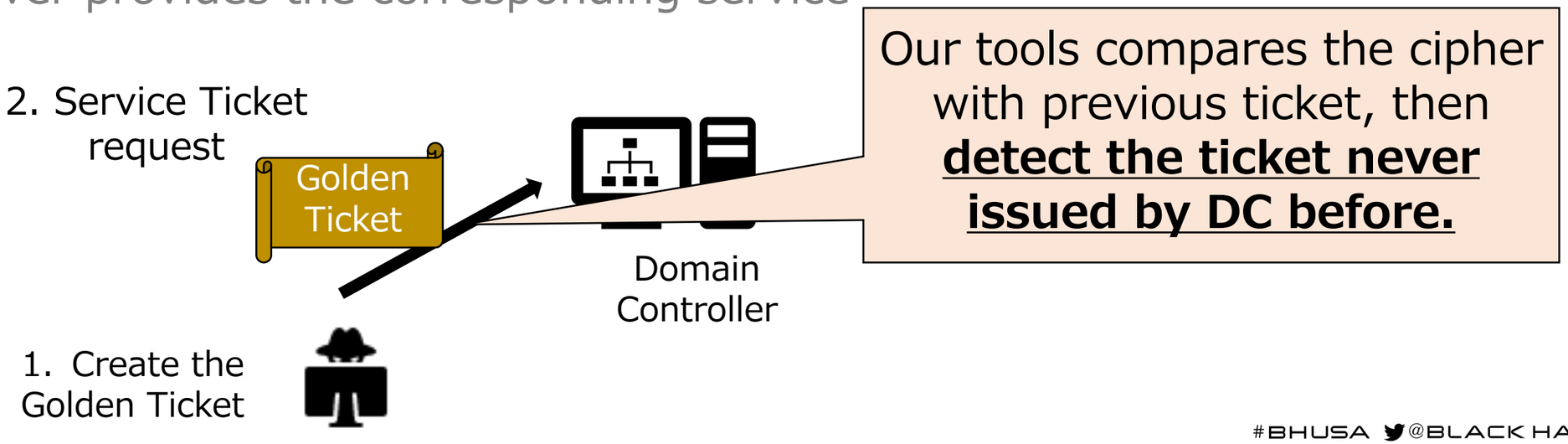






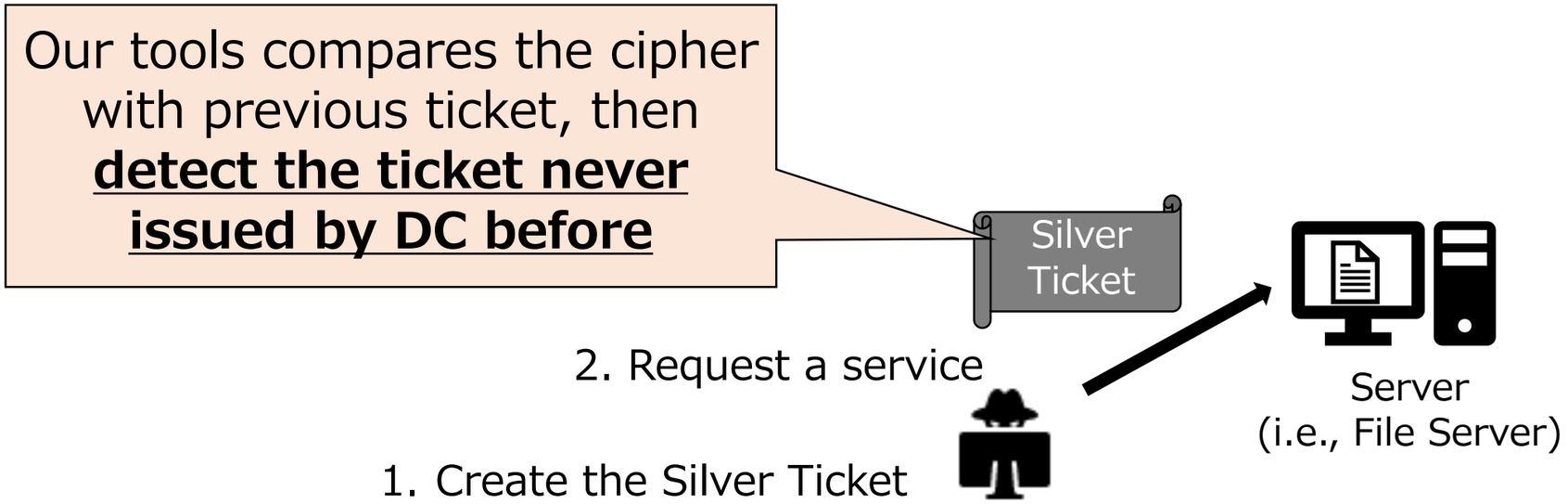
The use of the Golden Ticket

1. The attacker create the Golden Ticket
2. **The attacker requests Service Ticket to Domain Controller with Golden Ticket**
3. Domain Controller issues an encrypted Service Ticket
4. The user requests the server to use a service with Service Ticket
5. The server provides the corresponding service



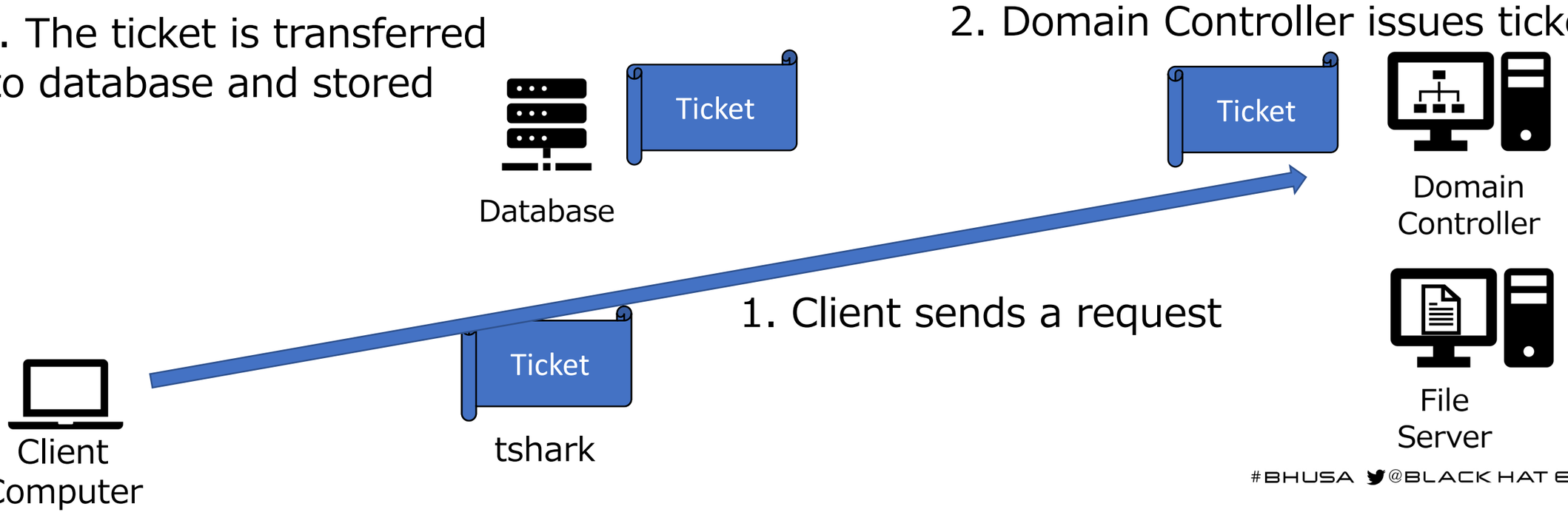
The use of the Silver Ticket

1. The attacker creates the Silver Ticket
2. **The attacker requests the server to use a service with Silver Ticket**
3. The server provides the corresponding service



Flow of detection with packet data

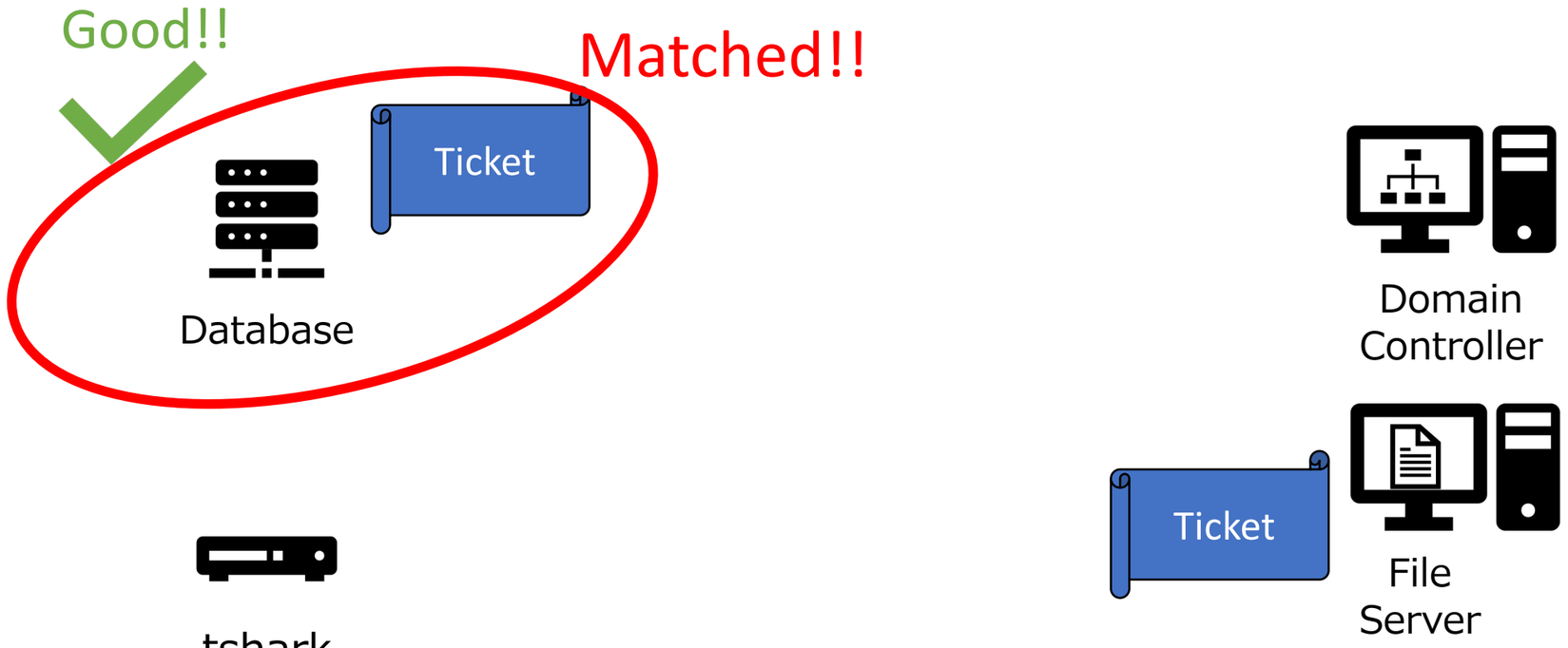
- We extracts tickets (Kerberos cipher) issued by DC using tshark (packet capturing software)
- The **Kerberos cipher issued by Domain Controller is stored into the database**
- We **compare Kerberos cipher included in client requests with ciphers in database**



Flow of detection with packet data

- If the Kerberos cipher is already stored in the database, judge it as “normal”

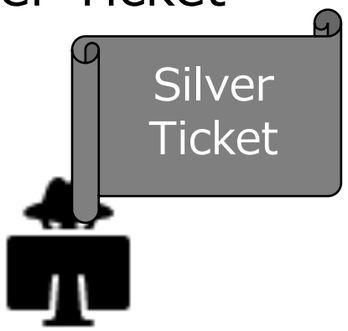
1. The client uses the ticket to access the file server



Flow of detection with packet data

- If Kerberos cipher is not stored in the database (=unknown cipher), it means the Golden / Silver Ticket is used

1. Attacker create the Silver Ticket

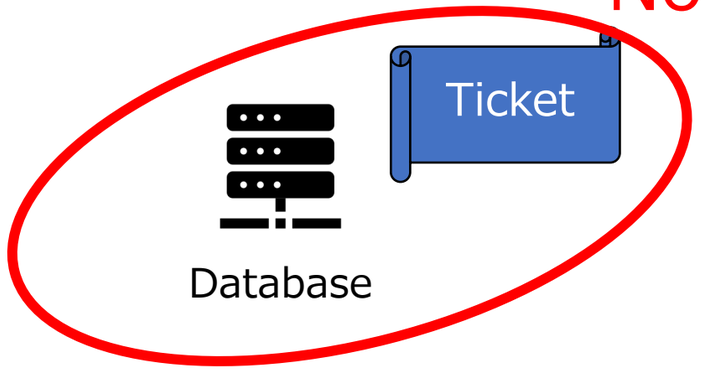


Attacker

Attack detected!!

2. The cipher of Silver Ticket does not match since the Domain Controller did not issue it before

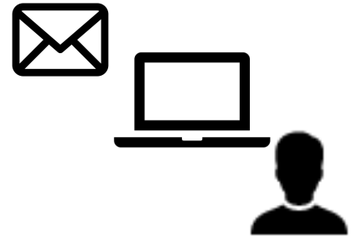
Not matched!!



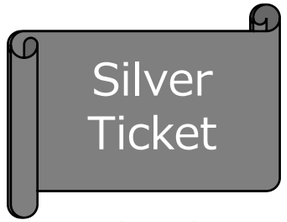
Database

Domain Controller

3. Send alert mail



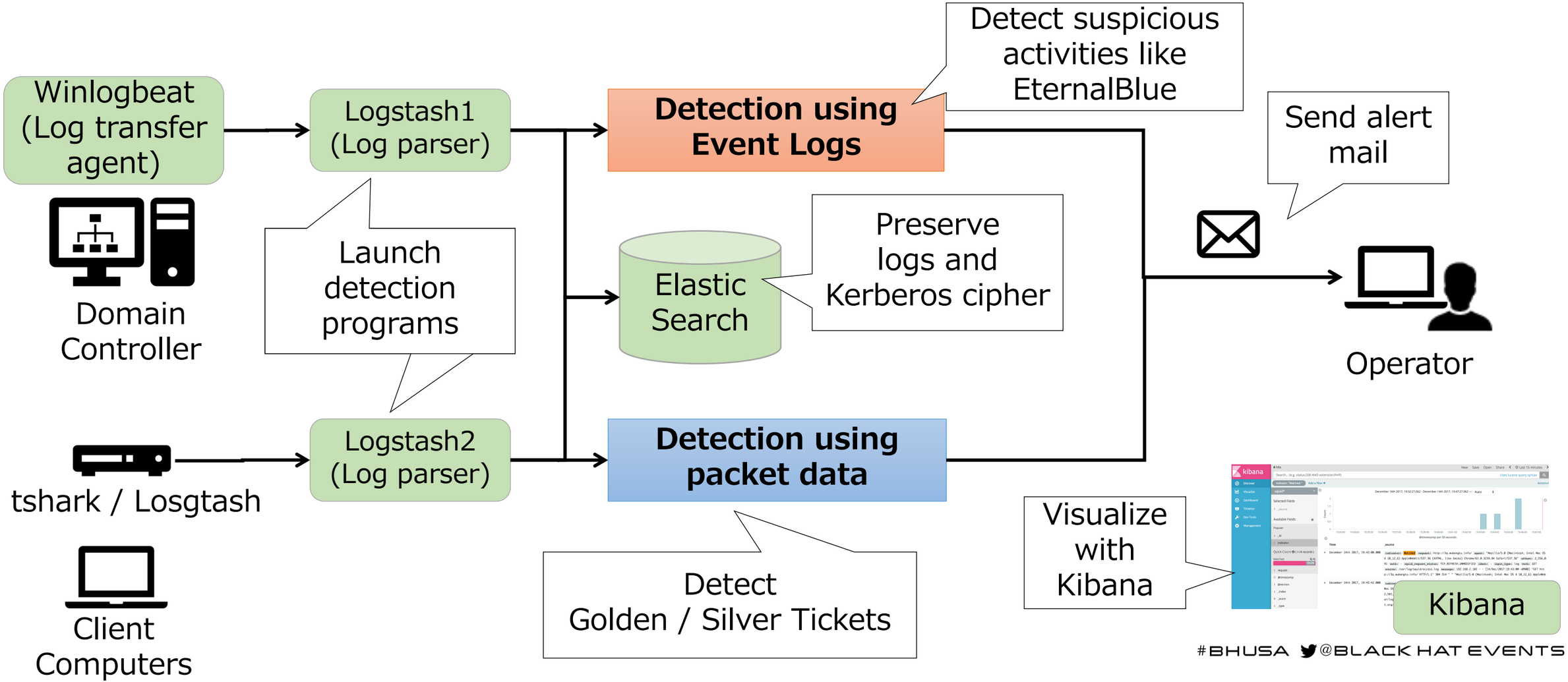
Client Computers



tshark

File Server

Implementation of our tools



Demonstration Scenario

1. Get administrative privilege on Domain Controller using Eternal Blue
2. Steal credentials to create the Golden / Silver Ticket
3. Create the Golden / Silver ticket (skip in this demo.)
4. Access the Domain Controller with the Golden Ticket disguising themselves as “dcadmin (legitimate Domain Administrator)”
5. Access the file server with the Silver Ticket disguising themselves as “fileadmin (legitimate administrator of the file server)”

We published the sample code of our tool.

https://github.com/sisoc-tokyo/Real-timeDetectionAD_ver2

Thank you for your attention!

coe@sisoc.org