

Detecting Lateral Movement in APTs

~Analysis Approach on Windows Event Logs~

June 17, 2016

Shingo ABE

ICS security Response Group

JPCERT/CC

Agenda

- Introduction to JPCERT/CC
- About system-wide intrusions
- Analyzing Windows event logs
- Conclusion

Self-introduction

Shingo Abe

Information Analyst at
ICS security Response Group,
JPCERT/CC since 2014.

- In the past...
 - Implementation of a cryptographic algorithm
 - Mobile Device Management (MDM)
 - Developed key management system
 - etc
- Now...
 - ICS security
 - IoT security
 - Log analysis
 - etc



About JPCERT Coordination Center

- Foundation
 - October, 1996
- Organization Status & Constituency
 - An independent, non-profit organization
 - Internet users in Japan, for enterprises
 - Mainly providing service through technical staffs with high degree of professionalism in enterprise
- International and Regional Activities



JPCERT/CC - 3 Services and 6 Basic Activities -



Early Warning Information	Information sharing with critical infrastructure enterprises, etc.
CSIRT Establishment Support	Capacity building for internal CSIRTs in enterprises / overseas national CSIRTs
Industrial Control System Security	Activities to protect ICS, such as incident handling and information gathering / sharing
Artifact Analysis	Analysis on attack methods / behavior of malware (unauthorized program)
Domestic Collaboration	Collaboration with various security communities in Japan
International Collaboration	Collaboration with overseas organizations for smoother handling of incidents and vulnerabilities

Assigned by METI as the vulnerability handling organization.

About the Industrial Control Systems security Response Group

■ Industrial Control Systems security Response group (ICSR)

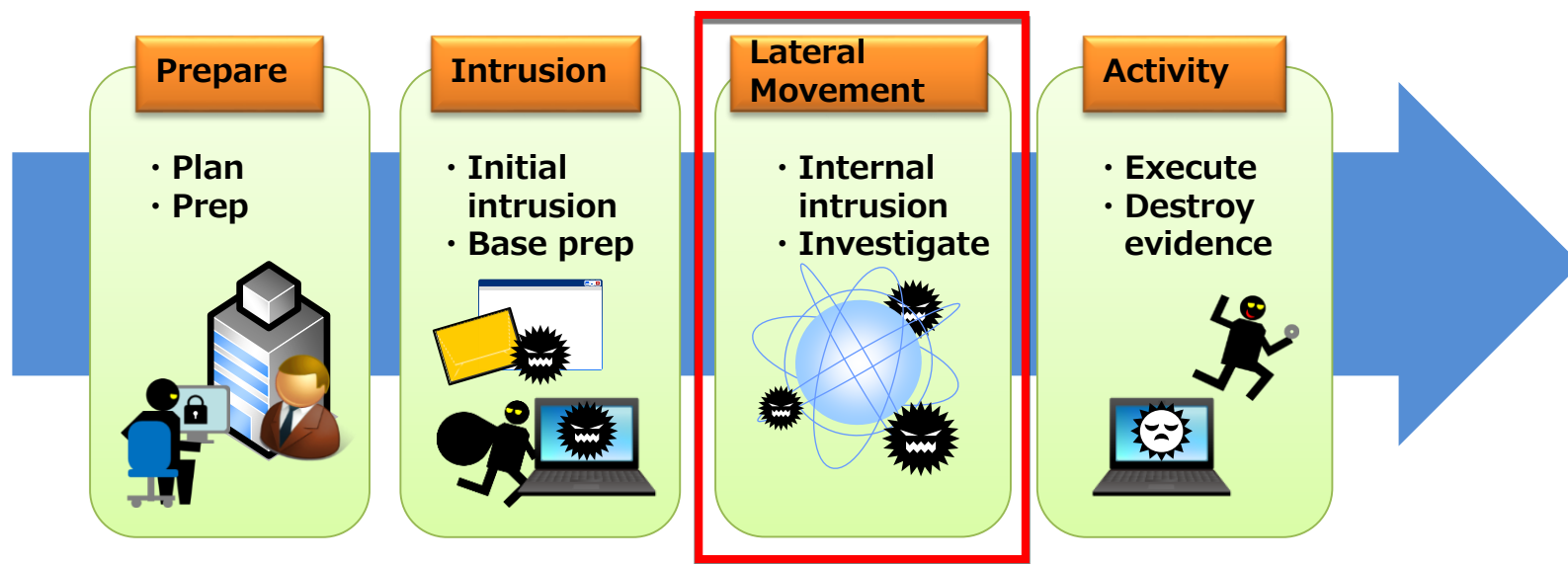
- JPCERT/CC created a dedicated team for "Control Systems Security Response" in the summer 2012
 - Activities related to controls systems security originally started at JPCERT/CC in 2007
- Main activities include:
 1. Reception of ICS incident reports and provide response assistance
 2. Vulnerability handling of ICS related products
 3. Collect / Analyze / Transmit information related to ICS security
 4. Provide self-assessment tool (J-CLICS/SSAT)
 5. Public Awareness, Collaboration
 - Hold an annual control systems security conference
 - Administration of various communities

Etc.
- In the US, ICS-CERT exists and specializes in control systems (since 2009)

ABOUT SYSTEM-WIDE INTRUSIONS

Background

- Targeted attacks today are becoming more sophisticated and it is difficult to completely prevent attacks by just defending the border
- Attackers remain within the systems of an organization and cleverly steal information over a long period of time
- If detection is delayed, damages increase. It is critical to detect as soon as possible to stop the attack.

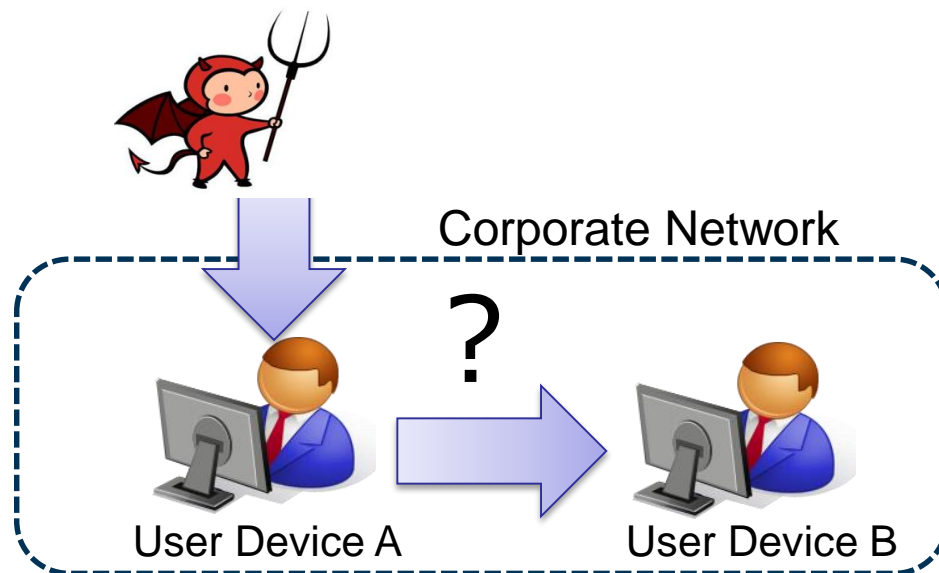


Today's focus

System-wide intrusions explained

- Attackers attempt to spread infections to achieve their goals or search for information that may be of value
- To spread infections within the system, attackers may use the following methods (for lateral movement)
 1. Unauthorized use of domain administrator account
 2. Unauthorized use of Local Admin account
 3. Replacing files on a server in an unauthorized manner

Focus here

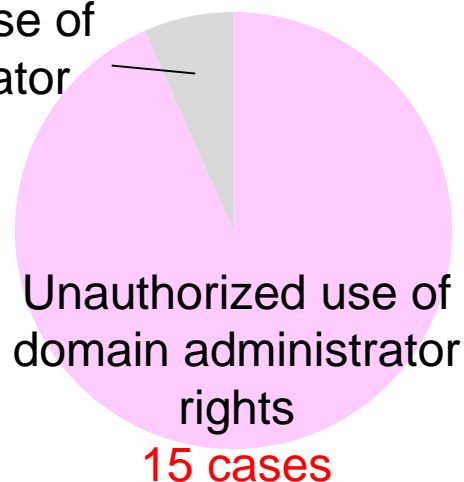


Number of confirmed cases for unauthorized use of domain administrator rights

Out of the targeted attacks cases handled during FY 2015 at JPCERT/CC, the number of cases (relatively clearly) confirmed where attack activity (system-wide intrusion) was on-going within the target network

16 cases

No unauthorized use of domain administrator rights
1 case



Cause for unauthorized use

Unknown
4 cases

Password obtained
5 cases

AD vulnerability +
Password obtained
6 cases

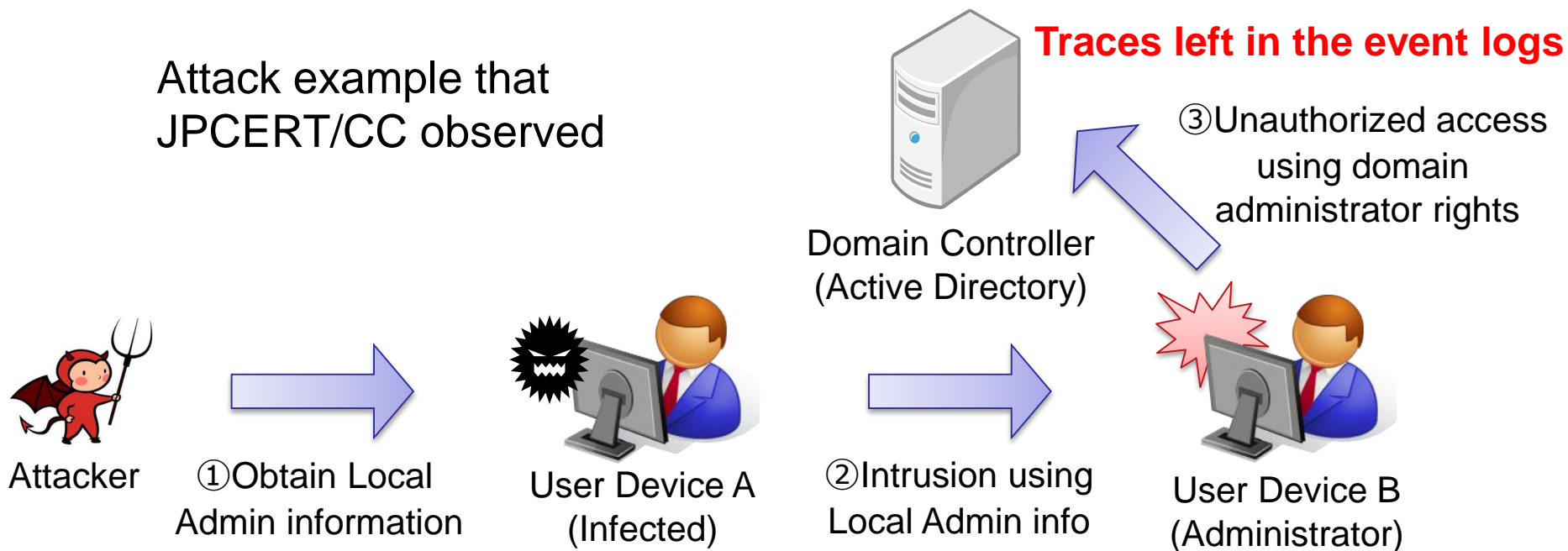
- After intrusion, almost all cases (15 / 16) resulted in unauthorized use of domain administrator account
- Almost half of the Domain Controllers (Active Directory) were not updated to address known vulnerabilities

[Case Study]

Unauthorized use of domain administrator account

- Domain administrators **have rights that allow them to perform various operations**, thus become a target for attackers
- Methods used to steal domain account administrator rights include:
 - Exploit vulnerabilities in Active Directory
 - Use local device registry keys, domain administrator account password hash values stored on memory

Attack example that
JPCERT/CC observed



ANALYZING WINDOWS EVENT LOGS

Motivation behind the analysis and considerations

■ Motivation

- To more effectively discover system-wide intrusions in traditional IT systems as part of incident response by narrowing analysis targets to specific events and fields

■ Method Considerations

- In order to control a device from another device within the same domain, authentication via Kerberos or NTLM is required
 - If authentication is performed, **event IDs related to the authentication** are recorded in the Domain Controller
 - Events related to authentication contain fields for **device requesting authentication** and **administrator account**

What event IDs to look for in the target?

- Perform an investigation targeting the following event IDs:
 - Successful Login (Event ID:4624)
 - Failed Login (Event ID:4625)
 - Kerberos Authentication (Event ID:4768)
 - Kerberos Service Ticket (Event ID:4769)
 - NTLM Authentication (Event ID:4776)
 - Assignment of Administrator Rights (Event ID:4672)

* These event IDs are for Windows Vista / Server 2008 and later

Event IDs and Fields to be extracted

Successful Login (4624), Failed login (4625)

	Event Log Item Name
Time	
Account Name	New Logon: Account Name:
Device Requesting Authentication (IP Address)	Network Information: Source Network Address:
Device Requesting Authentication (Host Name)	Network Information: Workstation Name:
Error Code ※4625 only	Failure Information: Status:

NTLM Authentication(4776)

	Event Log Item Name
Time	
Account Name	Logon Account:
Device Requesting Authentication (Host Name)	Source Workstation:
Result Code	Error Code:

Kerberos Authentication(4768), Kerberos Service Ticket (4769)

	Event Log Item Name
Time	
Account Name	Account Information: Account Name:
Device Requesting Authentication (IP Address)	Network Information: Client Address:
Result Code	Additional Information: Result Code:

Assignment of Administrator Rights(4672)

	Event Log Item Name
Time	
Account Name	Account Name:

Analysis results to output

- List of devices that use domain administrator accounts
- Relationship between domain administrator account and devices that requested authentication
 - To check the validity of the devices that use domain administrator accounts

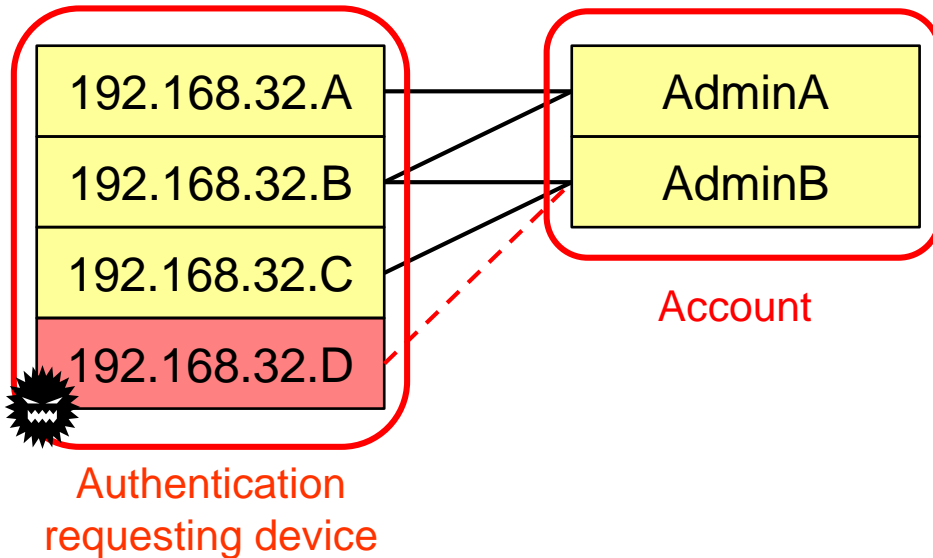
- The number of authentication attempts per day for each domain administrator account
 - To check for sudden changes in the number of authentication attempts or accounts not typically used during certain periods of time

- List of users with specialized rights
 - To check for uses of such special rights by accounts that do not normally use these rights

Sample of results output

- By visualizing the relationship between the devices requesting authentication and domain administrator account, dates and number of authentication attempts, validity can be easily checked for

Devices requesting authentication and domain administration accounts



Devices requesting authentication and number of authentication attempts

		2016/06						
		01 WED	02 THU	03 FRI	04 SAT	05 SUN	06 MON	07 TUE
AdminB	4624	5	8				11	6
	4625							
	4768							
	4769							
	192.168.32.C	4776	5	13			7	6
192.168.32.D	4624		1		32	14		
	4625		20					
	4768				30	18		
	4769			123				
	4776							

Applying to investigate incidents in control systems

- Motivation behind applying this method to control systems
 - In traditional IT systems, we were able to discover other infected devices and accounts being maliciously used during incident response
 - For the following reasons, we thought that this method could be useful in control systems that do not use AD:
 1. Devices and administrator accounts used in control systems are limited
 2. The number of total events should be lower than traditional IT systems, so anomalies should be relatively easy to detect
 3. Does not require implementing a new "security device"

- With cooperation from some asset owners, we were able to obtain logs for critical Windows devices (OPC server, etc.) used in control systems and applied this analysis method

The effectiveness of this method

■ Effectiveness of this method

- Utilize for re-examining operations
 - Grasp behavior that differs from the norm
 - Optimize and minimize the number of devices that use administrator accounts
- Utilize for re-examining log settings
 - Settings for size and rotation of logs
 - Settings for audit policies

Audit policies that should be in place

■ Account logon

- Audit to check credential information
- Audit for Kerberos authentication service

■ Log on / Log off

- Audit logons
- Audit other logon / log off events
- Audit special logons

✘ Enabled by default in Windows Server 2008 / 2012

Some remaining challenges

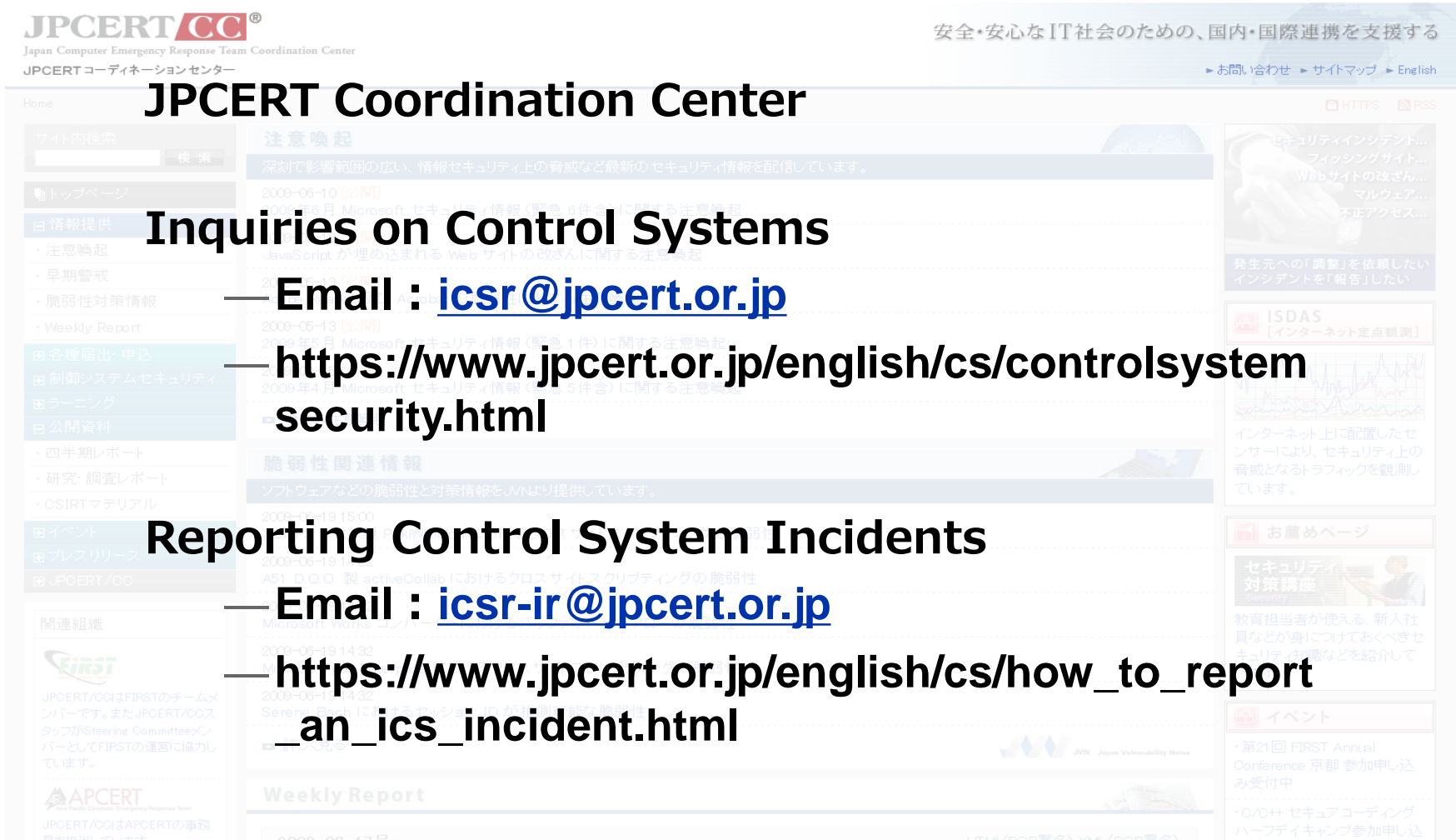
- When blended in with legitimate authentications, unauthorized use is hard to recognize
- If there are complexities between the device requesting authentication and the administrator account, it is difficult to determine validity
- In DHCP environments, devices cannot be identified using IP addresses alone, therefore it is necessary to use DHCP logs

CONCLUSION

Conclusion

- Introduced an analysis method to discover system-wide intrusions
- Was useful in discovering (unauthorized use of devices and accounts) system-wide intrusions during incident response in traditional IT systems
- Applying the method to Windows devices in control systems left us with a good impression going forward
- The next step is apply the method against logs after an incident in a control system
- Looking for partners that may be willing to provide logs for this analysis!

For Inquiries and Incident Response Requests



The screenshot shows the JPCERT/CC website interface. At the top left is the JPCERT/CC logo and the text "Japan Computer Emergency Response Team Coordination Center" and "JPCERT コーディネーションセンター". At the top right is the slogan "安全・安心なIT社会のための、国内・国際連携を支援する" and navigation links for "お問い合わせ", "サイトマップ", and "English". The main content area features a search bar, a "注意喚起" (Attention) section with a date of 2008-06-10, and a "脆弱性関連情報" (Vulnerability Related Information) section. On the right side, there are several widgets including "セキュリティインシデント...", "ISDAS [インターネット定点観測]", "お読みページ" (Read Page) for "セキュリティ対策講座", and "イベント" (Events) listing the "第21回 FIRST Annual Conference 京都 参加申し込み受付中".

JPCERT Coordination Center

Inquiries on Control Systems

- Email : icsr@jpcert.or.jp
- <https://www.jpcert.or.jp/english/cs/controlsystem-security.html>

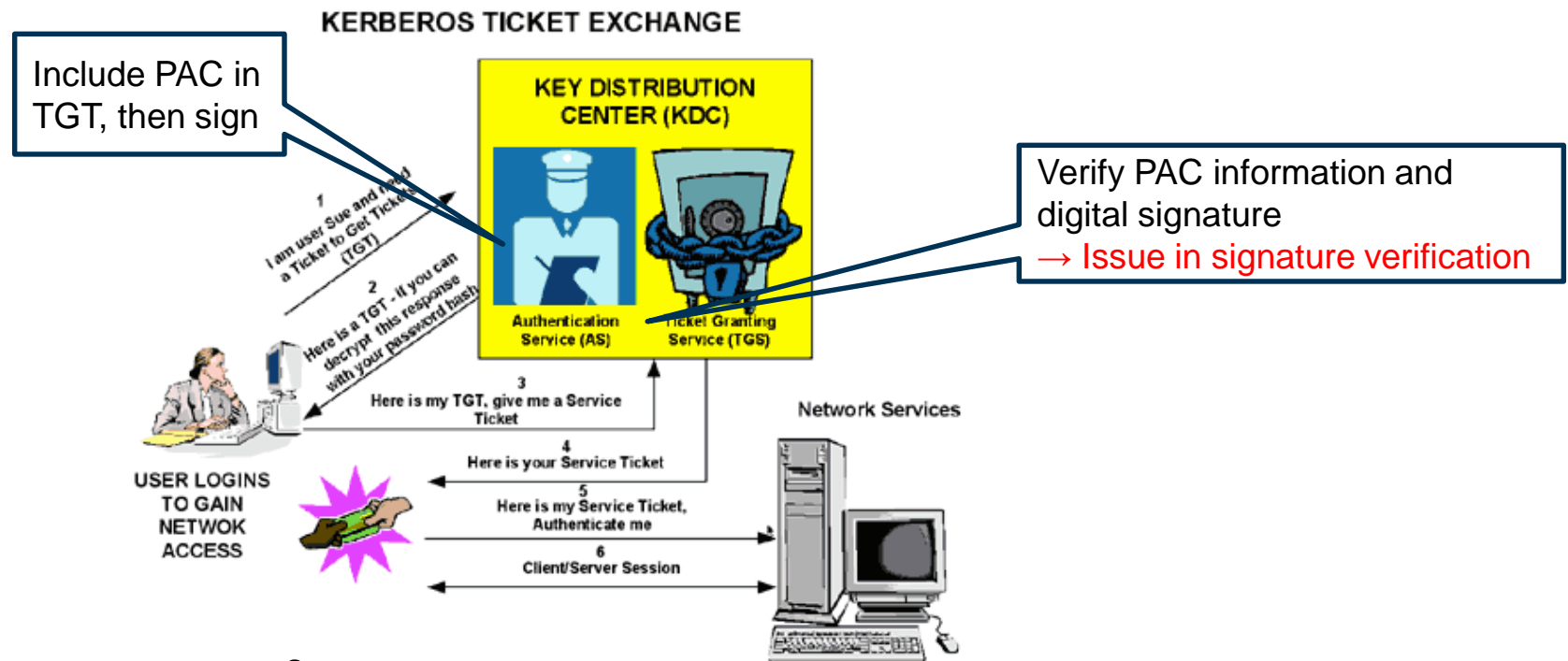
Reporting Control System Incidents

- Email : icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

Thank you for your attention

Details on Kerberos KDC vulnerability

- Vulnerability where service ticket is issued without properly verifying the PAC (Domain SID and affiliated security group) digital signature when KDC receives TGT ticket
 - Attacker can alter data related to rights within PAC, which may result in assigning itself as part of the domain administrator group

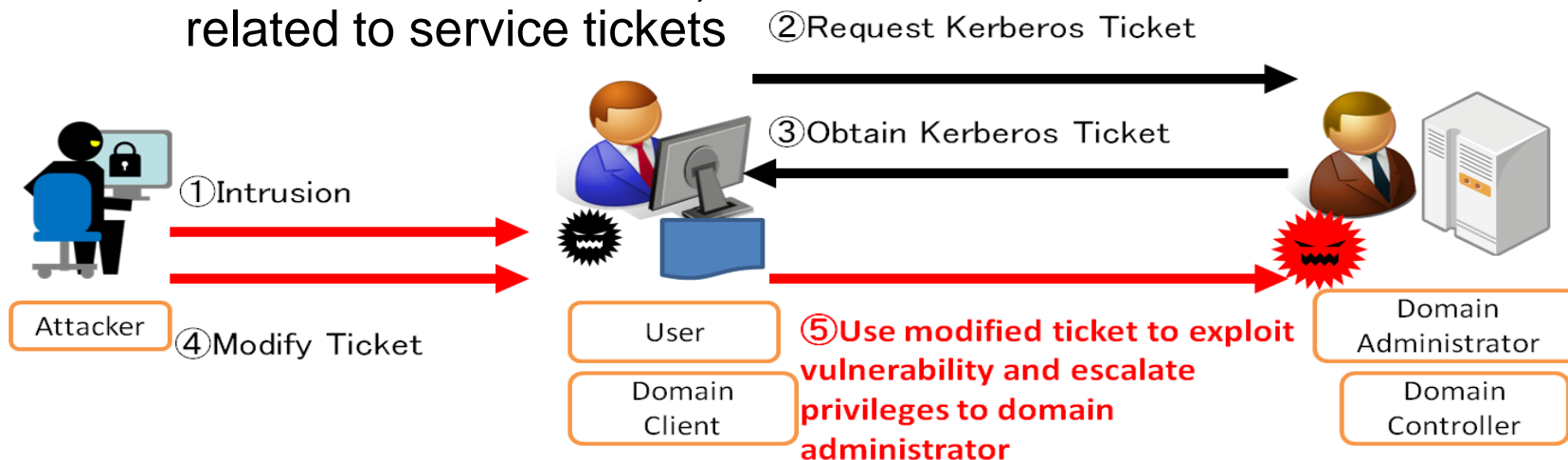


Source:

<http://blogs.technet.com/b/srd/archive/2014/11/18/additional-information-about-cve-2014-6324.aspx>

Analysis overview of Kerberos KDC vulnerability

- Check whether there are event outputs when an attack exploiting the Kerberos KDC vulnerability (CVE-2014-6324) to escalate privileges to domain administrator
 - Prior to applying patch
 - Check whether there are special rights assigned to accounts that are not domain administrators (Event ID: 4672)
 - After applying patch
 - Check whether there are authentication failures (Event ID: 4769, Failure Code:0xf) related to service tickets



Overview of attack exploiting Kerberos KDC vulnerability

Method to determine whether administrator account is being used appropriately

- The left example can be determined as standard use since authentication for the administrator account is being performed from the AD administrator device (192.0.2.20).
- The right example can be determined as unauthorized use since authentication for the administrator account is being performed from a device (192.0.2.40) that is not normally used for authentication

• Appropriate account use / management

Active Directory(DC)
(192.0.2.10)



2. Issue authentication ticket



1. Request authentication ticket
using the administrator account

3. Login using the ticket



AD Administrator
(192.0.2.20)

Target Managed Device
(192.0.2.30)

• Unauthorized account use by attacker

Active Directory(DC)
(192.0.2.10)



Intruded device
(192.0.2.40)



2. Issue authentication ticket

1. Request authentication ticket
using stolen administrator
account

3. Login using the ticket



AD Administrator
(192.0.2.20)



Target Managed Device
(192.0.2.30)

Authentication information stored in memory of Windows devices

OS Version	User	Kerberos	Hash		Plaintext Password
		TGT	LM	NTLM	
Windows Server 2003 Windows Vista and before	Local	Not saved	Saved	Saved	Saved
	Domain	Saved	Saved	Saved	Saved
Windows Server 2008R2 Windows 7	Local	Not saved	Not saved※1	Saved	Not saved※1
	Domain	Saved	Not saved※1	Saved	Not saved※1
Windows Server 2012R2 Windows 8.1	Local	Not saved	Not saved	Saved※2	Not saved
	Domain	Saved※2	Not saved	Saved※2	Not saved
	Protected User	Saved※2	Not saved	Not saved	Not saved
	Restricted Admin	Not saved	Not saved	Not saved	Not saved

※1 : Requires security update (KB2871997)

※2 : Protected by LSA Protection (function that prevents reading of memory by processes without MS signatures)

※ : Some authentication packages, such as digest require plaintext passwords and may be stored

Security has been enhanced since Windows 2012R2 / Win 8.1

(Ref) AD authentication events (for Windows 2003)

- Relationship between event IDs for Windows 2008 and later and 2003

	2008 and later	2003	Notes
Successful Login	4624	528(local login) 540(network login)	After 2008, "logon type" is used to identify
Failed Login	4625	529-537,539	In 2003, different IDs for each failure reason After 2008, "status code" is used to identify
Kerberos Authentication	4768	672(success) 676(fail)	After 2008, "result code" is used to identify
NTLM Authentication	4776	680	According to Microsoft, NTLM authentication is also recorded in 528 and 520, there is no additional information that can be obtained from 680
Assignment of administrative rights	4672	576	