SecurityInfo

Best Practices

 Issue
 02

 Date
 2024-09-26





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

- Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China Website: https://www.huawei.com
- Email: <u>support@huawei.com</u>

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page: <u>https://securitybulletin.huawei.com/enterprise/en/security-advisory</u>

Contents

1 Best Practices for Using Huawei Accounts	1
2 Best Practices in Enabling High-Risk Ports	7
3 Disposal of Spam Mails Sent to External Systems	13
3.1 What Is Spam Email and How It Is Harmful	13
3.2 How Huawei Cloud Handles Resources That Send Spam Email	14
4 UDP-based Amplification Attack Check	15
4.1 Overview	
4.2 Detecting UDP-based Amplification Attacks	16
4.3 Solution and Prevention Measures	
5 Host Security Checks	
5.1 Hosts Security Issues	
5.1.1 Overview	
5.1.2 External Attacks: Port Scan	
5.1.3 Mining	
5.1.4 Ransomware	21
5.2 Host Security Check (Windows)	
5.2.1 Troubleshooting Methods	22
5.2.2 Troubleshooting Process	22
5.2.2.1 Method 1: Using Tools to Detect Security Issues	
5.2.2.1.1 Step 1: Analyzing All Processes	22
5.2.2.1.2 Step 2: Detecting Automatic Startup Programs	25
5.2.2.1.3 Step 3: Analyzing the Network	
5.2.2.1.4 Step 4: Detecting Abnormal Users	
5.2.2.2 Method 2: Using DOS System Commands to Check Processes	
5.2.2.3 Security Hardening Suggestions for Windows Hosts	
5.3 Host Security Check (Linux)	
5.3.1 Troubleshooting Methods	
5.3.2 Troubleshooting Process	37
5.3.3 Security Hardening Suggestions for Linux Hosts	

Best Practices for Using Huawei Accounts

To safeguard your Huawei Cloud accounts and help you set up a secure channel to access Huawei Cloud resources, we recommend the following settings on IAM.

Enabling Login Protection

After login protection is enabled, you and users created using your account will be authenticated by a virtual MFA device, SMS, or email during console login. This improves account security and prevents phishing attacks or accidental password leakage.

Step 1 Enable login protection for the account. **Table 1-1** shows an example.

User Roles	Procedure
Huawei Cloud Account	Go to the Security Settings page. Select Critical Operations > Login Protection, click Enable. In the displayed pane, select Enable.

Table 1-1 User roles

NOTE

- Your Huawei Cloud account is created after you successfully register with Huawei Cloud. Your account has full access permissions for your cloud resources and makes payments for the use of these resources.
- Your HUAWEI ID is a unified identity that you can use to access all Huawei services.

Step 2 Enable login protection for each IAM user under your Huawei Cloud account.

 Choose Identity and Access Management > Users and click Security Settings in the row where an IAM user resides.

Figure 1-1 Users

IAM	Users ⑦					G Feedback	Create User
User Groups	IAM User Login Link: https://auth.huaw Defete Modify Users	elcloud.com/aut2 🗗 available for creation: 9			Username • Enter a use	mame.	Q @
Permissions -	Username ↓≡	Description JE	Status ↓Ξ	Last Login ↓≡	Created 4F	Operation	
Projects			Enabled	Dec 05, 2022 21:04:02 GMT+08	Dec 05, 2022 15:04:58 GMT+08:	Authorize Modify More	•
Agencies			 Enabled 	Dec 09, 2022 10:17:21 GMT+08	Nov 11, 2022 14:20:41 GMT+08:00	Aut Delete	
Identity Providers	□ y >0	-	Enabled	Dec 06, 2022 10:38:37 GMT+08	Oct 24, 2022 16:58:36 GMT+08:00	Authorize moany more -	
Security Settings	□ ¥ □	-	Enabled		Oct 14, 2022 16:15:37 GMT+08:00	Authorize Modify More +	
	t 4	-	Enabled	Oct 29, 2022 19:54:41 GMT+08:00	Oct 09, 2022 16:58:14 GMT+08:00	Authorize Modify More +	

2. Click \checkmark in the Login Protection area.

Figure 1-2 Security Settings

Basic Information	User Groups	Security Settings
MFA Authentication		
SMS	$(a,b) \in [a,b]$	
Email Address	and the second	
Virtual MFA Device	🌖 Unbound ၇	
Login Credentials		
Login Password	Strong 🖉 Last Pass	word Change Jun 01, 2021 10:10:21 GMT+08:00
Login Protection ⑦		
Verification Method	Disabled	

3. In the displayed **Change Verification Method** dialog box, select **SMS**, **Email**, or **Virtual MFA device** for **Verification Method**, and click **OK**.

Figure 1-3 Change Verification Method

Change Verificatio	on Method	×
Username		
Verification Method	SMS Email Virtual MFA device Disabled	
	OK Cancel	

----End

Enabling Critical Operation Protection

After critical operation protection is enabled, if you or users created using your account perform a **critical operation**, such as deleting a resource and generating an access key, a password and a verification code are required for additional authentication. This prevents risks and loss caused by misoperations.

- Step 1 Go to the Security Settings page as the administrator.
- **Step 2** Select **Critical Operations**, locate the **Operation Protection** row, and click **Enable**.

Figure 1-4 Critical Operations

Security Settings 🕐	
Basic Information Critical Operations Login Authentication Policy Password Policy ACL	
Virtual MRA Docke Too can use the virtual MRA device bound to your account to authenticate console logins. Coversional the <u>HERREEL COURD are</u> or an authenticator app on your mobile plone and bind it to your account.	A Unbound Bind
Login protection Login protection enhances the security of your account and cloud services.	A Disabled Enable
Operation Protection Operation protection authenticate you and users cruated using your account by a vitual MPA device, SMS, or email before allowing ortical consele operations such as deleting an ECS or writinging as EDP Learn more	A Disabled Enable
Access Key Management. It is folded, and all the over under your account can manage tomate, enable, divide, and delete) ther own access keys if you enable this option, only the administrator can manage access keys of access.	▲ Disabled

- **Step 3** On the displayed pane, select **Enable** for **Operation Protection**. Then, select **Self-verification** or **Verification by another person**.
 - **Self-verification**: You or IAM users themselves perform verification when performing a critical operation.
 - Verification by another person: The specified person completes verification when you or IAM users perform a critical operation. Only SMS and email verification is supported.

peration Protection	1 / • / • / • •			
Operation protection p	rovides an additional la	yer of securit	y for cloud	resources
You and users created using email bef	your account will be authe ore being allowed to perfo	enticated by a vi rm a critical ope	rtual MFA de ration.	evice, SMS,
Operation Protection	Enable You and users created to perform identity verific here.	using your accou ation by using th	int will need ne method y	to ou specify
	 Self-verification Verification by ano Specify a mobile numb 	ther person	rification	
	+86 (Chinese V	Enter a mobil	e number.	
]	1	
	6-digit code		Send Co	de
	Email Address Verificat	ion		
(Disable Identity verification will critical operation. 	l not be required	l for perform	ing a
		_		

. . . **۔**: ـ _. _



----End

Configuring a Login Authentication Policy

A login authentication policy includes many aspects of account security, including session timeout, account lockout, recent login information, and custom login

prompt. You can configure a login authentication policy to better safeguard your account, preventing password leakage caused by forgetting to log out or phishing attacks.

- Step 1 Go to the Security Settings page as the administrator.
- **Step 2** Select **Login Authentication Policy** and configure required parameters as shown in the following figure.

Figure 1-6 Login Authentication Policy

Secu	rity Settings ⑦				
	Basic Information	Critical Operations	Login Authentication Policy	Password Policy	ACL
	Session Timeout	6 J. 111 .			
	Log out if no operati	ons are performed within 1	hours •		
	Account Lockout	Takes effect for both you and	I IAM users created using your account		
	Lock the account for	15 minutes if 5	login attempts fail within 15 mir	nutes.	
	Account Disabling	Takes effect only for IAM us upon login if it is not used wi	sers created using your account thin the validity period		
	Recent Login Info	rmation			
	🔽 Display last logii	n information upon successful	login		
	Custom Informati	on			
	Display custom infor	mation upon login.			
	welcome		A		
			7/60		
	Save				

NOTE

You can provide your custom information which will be displayed when you log in.

----End

Configuring Password Policies

You can specify minimum password length, restrict consecutive identical character, and disallow previously used passwords to ensure that strong passwords of high complexity are used.

Step 1 Go to the Security Settings page as the administrator.

Step 2 Select **Password Policy** and configure required parameters as shown in the following figure.

urity Settings ⑦				
Basic Information	Critical Operations	Login Authentication Policy	Password Policy	ACL
Password Compos	ition & Reuse			
Must contain at leas	t 3 of the following ch	naracter types: uppercase letters, lower	case letters, digits and spe	cial chara
Minimum Number o	f Characters 8			
Restrict consecut	tive identical characters			
Disallow previou	isly used passwords			
Number of Recent Pa	asswords Disallowed 5			
Password Expiration	on			
Prompt passwor	d change 15 days before expi	iration and force password change upo	n expiration	
Password Validity Pe	riod (days) 90			
Minimum Passwo	rd Age			
Allow a passwor	d to be changed only after it	is used for a specified time		

----End

2 Best Practices in Enabling High-Risk Ports

To safeguard your Huawei Cloud resources and help you set up a secure access channel to your Huawei Cloud resources, we recommend the following security policies for enabling high-risk ports.

Configuring Security Groups and Network ACL to Control Inbound Access

You can configure inbound rules in security groups and network ACLs to protect the ECSs in the security group and the subnets associated with the network ACL.

Step 1 Go to the Security Groups page.

- 1. Log in to the management console.
- 2. Click in the upper left corner of the management console and select a region and a project.
- 3. In the navigation pane on the left, click = and choose **Network** > **Virtual Private Cloud**.
- 4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
- **Step 2** Check each security group and delete high-risk port inbound rules.
 - 1. On the **Security Groups** page, locate a security group and click **Manage Rule** in the **Operation** column.

Figure 2-1 Security Groups page

Secur	ity Groups 💮					Peedback	(P Quick Links	Create Security Group
	Delete							c
	pecify filter criteria.							Q
	Name/ID		Security Group Rules	Associated Instances	Description	Enterprise Project	Operation	
		72-2e93a75a9841	5	6			Manage Rule	Manage Instance More +
1		31b-50c8c1f4ce17	4	0			Manage Rule	Manage Instance More +
		-a6-066232acfed2	7	0			Manage Rule	Manage Instance More +
1		+47a32e9c1632	4	4			Manage Rule	Manage Instance More +

2. Click the **Inbound Rules** tab, check for the protocols and ports listed in **Protocol & Port** in **Table 2-1**, and find the policy whose **Action** is **Allow** and **Source** is **0.0.0.0/0**.

Figure 2-2 Checking security group policies

Summary Int	emmary Erbourd Rules Outbourd Rules Associated Instances							
G Some sec	curity group rules will not take effect fo	or ECSs with certain specifications. Le	am more					×
Add Rule	Fast-Add Rule Delete	Allow Common Ports Inte	isand Rules: 10 Learn	more about security group configuration.				0
Specify lifer or	ileria.							Q
Priority	① T Action ①	T Protocol & Port 🕥	у туре	Source ()	Description	Last Modified	Operation	
0.1	Allow	TCP : 9449	IPv4	00000 ()	security group rules use	Jul 07, 2821 17:39:29 G	Modity Replicate Detete	
	Allow	TOP : 2222	IPv4	00000 ①	security group rules use	Jul 07. 2021 17:39:22 G	Modify Replicate Delete	
	Allow	44	19-4	00000 🖤		Jan 21, 2020 15:08:20	Muskly Replicate Delete	
	Allow	A8	iPv6	ot -any 🕥		Jan 21, 2020 15:07:35	Modity Replicate Delete	
	Allow	TCP: 00	1954	00000 ()		Jan 21, 2020 15:07:35	Modify Replicate Detete	
0 1	Allow	TOP : 445	iPv4	00000 3		Jan 21, 2020 15:07:35	Modify Replicate Delete	
	Allow	TCP 3389	1994	00000 1		Jan 21, 2020 15:07:35	Multy Replicate Detete	

Table 2-1 High-risk ports

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 20, 21	File Transfer Protocol (FTP)	TCP: 3306	MySQL (database)
TCP: 22	Secure Shell (SSH)	TCP: 3389	Windows Remote desktop protocol (RDP)
TCP: 23	Telnet (remote terminal protocol)	TCP: 3690	Subversion (SVN, an open-source version control system)
TCP: 25	Simple Mail Transfer Protocol (SMTP)	TCP: 4848	GlassFish (application server)
TCP/UDP: 53	Domain Name System (DNS)	TCP: 5000	Sybase/DB2 (database)
TCP: 69	Trivial File Transfer Protocol (TFTP)	TCP: 5432	PostgreSQL (database)
TCP: 110	Post Office Protocol 3 (POP3)	TCP: 5900-590 2	Virtual Network Console (VNC)
TCP: 111, 2049	Network File System (NFS)	TCP: 5984	CouchDB (database)
TCP: 137, 139, 445	Server Message Block (SMB) protocol (NetBIOS)	TCP: 6379	Redis (database)
TCP: 143	Internet Message Access Protocol (IMAP)	TCP: 7001-700 2	WebLogic (web app system)
TCP: 389, 636	Lightweight Directory Access Protocol (LDAP)	TCP: 7199, 7000, 7001, 9160, 9042	Apache Cassandra
TCP: 512-514	Linux rexec (remote login)	TCP: 7778	Kloxo (virtual host management system)

Protocol Port (1)	Service	Protocol Port (2)	Service		
TCP: 873	Rsync (data image backup tool)	TCP: 8000	Ajenti (Linux server management panel)		
TCP: 1194	OpenVPN (virtual private channel)	TCP: 8069, 10050-10 051	Zabbix (system network monitoring)		
TCP: 1352	Lotus	TCP: 8443	Plesk (virtual server management panel)		
TCP: 1433	SQL Server (database management system)	TCP: 8080, 28015, 29015	RethinkDB		
TCP: 1521	Oracle (database)	TCP: 8080-808 9	Jenkins and JBoss (application server)		
TCP: 1500	ISPmanager (server control panel)	TCP: 8088, 50010, 50020, 50030, 50070	Hadoop (distributed file system)		
TCP: 1723	Point-to-Point Tunneling Protocol (PPTP)	TCP: 8848, 9848, 9849, 7848	Nacos service		
TCP: 2082-2083	cPanel (VM control system)	TCP: 9080-908 1, 9090	WebSphere (application server)		
TCP: 2181	ZooKeeper (reliable coordination service for distributed systems)	TCP: 9200, 9300	Elasticsearch (Lucene search server)		
TCP: 2601-2604	Zebra (route)	TCP: 11211	Memcached (cache system)		
TCP: 3128	Squid (caching proxy)	TCP: 27017-27 018	MongoDB (database)		
TCP: 3311-3312	kangle (web server)	TCP: 50000	SAP Management Console		

Protocol Port (1)	Service	Protocol Port (2)	Service		
TCP: 8080	DisConf (distributed configuration management platform)	TCP: 60010, 60030	HBase		
TCP: 8888	Spring Cloud Config (distributed configuration center)	TCP: 3000	Grafana (data visualization)		
TCP: 8761	Eureka (service registration and discovery component)	TCP: 8983	Solr (open-source enterprise-search platform)		
TCP: 8500, 8502	Consul (service registration and discovery component)	TCP: 3123-312 4, 8081, 6123	Flink (big data processing platform)		
TCP: 8070, 8080	Apollo (distributed configuration management platform)	TCP: 4040, 7077, 8080-808 1	Spark (big data processing platform)		
TCP: 8090	Diamond (distributed configuration management system)	TCP: 8080, 11800, 12800	SkyWalking (distributed system monitoring)		
TCP: 2379-2380	Etcd (distributed key- value storage system)	TCP: 8080	WebTTY (Web TTY management page)		
TCP: 15672	RabbitMQ (message queue)	TCP: 80, 443	NextCloud (private network hard disk)		
TCP: 8161, 61616	ActiveMQ (message queue)	TCP: 9001, 9090	Minio (cloud storage management tool)		
TCP: 8083, 8086, 8635	InfluxDB (time series database)	TCP: 18083	EMQX (IoT access platform)		
TCP: 6030-6032, 6041	TDengine (time series database)	TCP: 1090, 1099	Java-RMI protocol (Java remote method invocation protocol)		
TCP: 9092-9095, 9999	Kafka (distributed stream processing platform)	TCP: 8000	JDWP (Java remote debugging interface)		
TCP: 2375	Docker (application container engine)	TCP: 8009	Tomcat AJP protocol (binary communication protocol)		

Protocol Port (1)	Service	Protocol Port (2)	Service		
TCP: 5601	Kibana (data visualization)	TCP: 8888	Jupyter Notebook (web applications for interactive computing)		
TCP: 177	xmanager/xwin (Linux remote GUI)	TCP: 6443, 8443, 10250-10 256	Kubernetes (container orchestration engine)		
TCP: 8081	Nexus (repository manager)	TCP: 80/443, 8080	GitLab (code hosting platform)		
UDP: 161, 162	Simple Network Management Protocol (SNMP)	TCP: 5555	ADB (Android debugging tool)		
TCP: 1883, 8883	MQTT (IoT message protocol)	TCP: 6000-606 3	X11 (Linux remote GUI)		
TCP: 8888	Napster (P2P file sharing protocol)	-	-		

3. Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

Figure 2-3 High-risk port policies for security groups

Priority (?)	∀ Action ⑦	Protocol & Port (?)	🗑 Туре	Source (?)	Description	Last Modified	Operation
1	Allow	TCP : 9443	IPv4	0.0.0.00 ()	security group rules use	Jul 07, 2021 17:39:23 G	Modify Replicate Delete
1	Allow	TCP : 2222	IPv4	0.0.0.00 ③	security group rules use	Jul 07, 2021 17:39:22 G	Modify Replicate Delete
1	Allow	All	IPv4	0 00000	-	Jan 21, 2020 15:08:29	Modify Replicate Delete

NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set Source to the IP addresses in the whitelist. For details, see Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group.
- You are not advised to enable high-risk port policies for all IP addresses.
- **Step 3** In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
- **Step 4** Check all the network ACLs that are enabled and associated with subnets. Delete high-risk port policies from the inbound rules.
 - 1. In the network ACL list, locate a rule and click **Manage Rule** in the **Operation** column.

Figure 2-4 Network ACL page



 Click the Inbound Rules tab, check for the protocols and ports listed in Protocol & Port in Table 2-1, and find the policy whose Action is Allow and Source is 0.0.0.0/0.

Figure 2-5 Checking network ACL policies

O Some security group rules will not take effect for EOSs with certain specifications. Learn more									
Add Rule Past-Add Rule Debte Allow Commin Ports Interand Rules 10 Learn more about security group configuration.									
								Q	
Boostly (D)	W Action (D)	W. Brostonese & Board (Ch.	W. Tunn	Nource (D)	Description	I and Marchinest	Ormania		
		,	0 1994	man do					
1	Allow	TCP : 9445	1950-6	00000 (2)	security group rules use	Jul 07, 2021 17:39:23 G	Modity Replicate Delete		
1.00	Allow	TCP (3333	(Pol	0.0.0.00	security group rules use	Jul 07, 2021 17:38:22 G	Musidy Replicate Detete		
1	Adams		1994	0.0.0.0		Jan 21, 2020 16 08:20	Muskly Replicate Delete		
1.00	Allow	A8	(Pvi)	oi		Jan 31, 2020 15:07:35	Musilly Replicate Delete		
1	Allere	TCP - 80	1994	0.0.0.0 D		Jan 21, 2020 15 07:35	Multy Replicate Delete		
1	Adams	TCP - 443	(Pv4	0.0.0.0 D		Jan 21, 2020 15 07:35	Muskly Replicate Delete		
	Allew	TCP : 3369	(Post	0.0.000 ①		Jan 21, 2020 15 07:35	Modity Replicate Delete		
	The security group take Practice Process T T T T T T T T T T T T T T T T T T	Comparison and a second s			Yes Yes Normality Name Yes Normality Normality Yes Normality Yes Normality Yes Normality Normality Yes Yes Normality Normality Normality Yes Normality Normality Normality Yes Normality Normality Normality Normality Yes Normality N	Number of the state o	Total State Total State Total State Total State Total State State	Terminal Part Part Control Part Part Part Part Part Part Part Part	

3. Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set Source to the IP addresses in the whitelist.
- You are not advised to open high-risk ports to all IP addresses.

----End

Using VPN/IPsec to Control Internal Access to Ports

By default, ECSs in a VPC cannot communicate with your physical data center or private network. To connect ECSs in a VPC to your data center or private network, you are advised to use Huawei Cloud Virtual Private Network (VPN).

Using Huawei Cloud Native Services to Enhance Security

Our cloud native services provide a range of features to enhance security.

Databases

Relational Database Service (RDS) provides a comprehensive performance monitoring system, implements a range of security measures, and offers a professional database management platform, allowing you to easily configure and scale databases on the cloud. On the RDS console, you can perform almost all necessary tasks and no programming is required. The console simplifies operations and reduces routine O&M workloads, so you can stay focused on application and service development.

Application middleware

Distributed Cache Service (DCS) provides **multiple features** to improve the reliability and security of tenant data, such as VPC, security group, whitelist, SSL encrypted connection for public network access, automatic backup, data snapshot, and cross-AZ deployment.

3 Disposal of Spam Mails Sent to External Systems

3.1 What Is Spam Email and How It Is Harmful

What Is Spam Email?

Spam email is unsolicited and unwanted junk email that is sent out in bulk to an indiscriminate recipient without the permission of the recipient. Usually, spam email always:

- Has no title, no sender, or source address.
- Has false information in the subject or content.
- Includes fraud information.
- Contains immoderate or illegal content.
- Hides harmful information such as viruses in the content.

How Is Spam Email Harmful?

Email is one of the important communication tools in today's society. Spam email will:

- Reduce communication quality: Spam email occupies a large amount of network bandwidth, affects the network transmission speed, and may cause mail server congestion.
- Damage the interests of the recipient: Spam usually contains hidden phishing links that may cause data leakage of recipients. Recipients may be then tricked into leaking credentials or business secrets. Spam email is repeated and spread quickly, it takes a lot of time and money for the recipient to stop it.
- Spread harmful information: Spam email is always used to spread harmful information such as rumors.

3.2 How Huawei Cloud Handles Resources That Send Spam Email

Overview

Using resources on Huawei Cloud to send spam email violates **Huawei Cloud User Agreement** and other related laws and regulations. IP addresses that are used to send out spam email in bulk will be recorded in the blocklist by the international anti-spam organization. IP addresses in the blocklist cannot be used for accessing websites, receiving emails, or sending emails. Once the IP address you obtained from Huawei Cloud is in the blocklist, the image of Huawei Cloud is servery damaged. If Huawei Cloud receives an external complaint that spam email is sent by resources of a Huawei Cloud user, Huawei Cloud will send a warning email to the user and take risk control measures (including but not limited to blocking ports and freezing IP addresses involved).

Rectification Suggestion

Huawei Cloud will implement risk control measures based on the complaint types.

You can open the **anti-spam organization** address, enter your IP address, and click **Start Testing** to check whether the IP address is listed by the organization as a spammer. Then handle the complaint accordingly.

Figure 3-1 Anti-spam organization

Test : IP 💙 value: 192.168.1.1 Start Testi
--

• If no IP address records are displayed on the page and the initial page is displayed, the IP address has not been blocked by the anti-spam organization.

Stop using the server with this IP address to send spam email as soon as possible and protect the mail address from malicious use. If the rectification is not completed within the time specified in the warning email, your resources may be blocked (including but not limited to blocking ports and freezing IP addresses).

• If your IP address is displayed on the page, the IP address has been blocked by the anti-spam organization.

The anti-spam organization has added your IP address to their blocklist. This means this IP address cannot be used to access websites or send emails anymore. Stop using this IP address to send spam email as soon as possible and protect your mail address.

Since the IP address blocklisted by the anti-spam organization is managed by Huawei Cloud, the image of Huawei Cloud is severely damaged. Huawei Cloud will permanently freeze the IP address. The IP address cannot be unfroze in any cases. Bind a new IP address to the server.

4 UDP-based Amplification Attack Check

4.1 Overview

What Are DDoS Attacks

DoS (Denial of Service) attacks are also called flood attacks. They are intended to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. A DDoS attack involves multiple compromised computers controlled by an attacker flooding the targeted server with superfluous requests.

What Are UDP-based Amplification Attacks

UDP-based amplification attacks are a form of DDoS attacks that are highly destructive, easy to trigger, and difficult to trace.

Figure 4-1 shows how such an attack works. An UDP-based amplification attack does not directly work on the target server. Instead, the attacker sends special UDP-based request packets to some open internet servers via IP addresses forged as that of the target server. These request packets will bring out high volumes of data to overwhelm the target server.

Figure 4-1 How a UDP-based amplification attack works



4.2 Detecting UDP-based Amplification Attacks

This section describes how to detect UDP amplification attacks on your sever.

1. Log in to the server as user **root**.

NOTE

In this example, the server sends ten 800-byte UDP packets per second when it is running properly.

2. Run the following command to check the current network connections and processes:

netstat -anput

You are advised to run the **netstat -anpt** command to check whether the current network connections and processes are normal. If the current connections and processes have been stopped or hidden, you can use the tcpdump packet capture tool to capture packets for analysis.

3. Run the following command to capture packets and analyze UDP traffic attacks:

tcpdump -nn udp

Figure 4-2 shows an example of the captured packets.

[root@ecs-9be0 tmp] \$ tcpdu	ump -nn udp "	
tcpdump: verbose output sup	pressed, use -v or	-vv for full protocol decode
listening on eth0, link-typ	e EN10MB (Ethernet)), capture size 262144 bytes
16:36:51.396455 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396473 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396475 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396478 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396480 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396483 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396485 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396487 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396490 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396492 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396495 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396497 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396500 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396502 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396505 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396507 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396509 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396512 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396514 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396517 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396519 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396521 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396524 IP	.32872 >	.19867: UDP, length 1460
16:36:51.396526 IP	.32872 >	.19867: UDP, length 1460

Figure 4-2 UDP attack packets

a. Run the following command to temporarily save the captured packet information to the **udp.pcap** file in the **/home** folder:

nohup tcpdump -nn udp -c 1000000 -w /home/udp.pcap &

b. Run the following command to analyze the captured packet information. **Figure 4-3** shows the analysis result.

tcpdump -nn -r /home/udp.pcap|awk -F'.' '{print \$1}'|sort|uniq -c

rigure 4 5 cuptured pucket undrysis result
[root@ecs-9be0 home] \$ tcpdump -nn -r /home/udp.pcap awk -F'.' '{print \$1}' sort uniq -c reading from file /home/udp.pcap, link-type EN10MB (Ethernet)
1701 16:40:45
55566 16:40:46
56007 16:40:47
55692 16:40:48
56272 16:40:49
55062 16:40:50
56007 16:40:51
55188 16:40:52
55944 16:40:53
56952 16:40:54
55818 16:40:55
56196 16:40:56
55188 16:40:57
55314 16:40:58
55629 16:40:59

Figure 4-3 Captured packet analysis result

According to step **3**, the checked device is sending dozens of 1460-byte UDP data packets to another IP address, which is far greater than the normal traffic. This indicates that the device is likely being used as an amplifier for UDP reflection attacks.

According to step **b**, the number of UDP connections per second is more than 50,000, indicating that the services provided by the device are used by attackers to launch UDP amplification attacks. So, necessary protection measures must be taken to prevent server resources from being exhausted by attack traffic.

4.3 Solution and Prevention Measures

You can take measures to defend against UDP amplification attacks based on service requirements. The following provides some recommended protection measures for your reference.

- Pay attention to the latest security advisories and bulletins released by security vendors, and implement targeted protection policies against such attacks in a timely manner.
- Use firewalls to control access to the UDP ports of ECSs.
- Configure security groups to control access to UDP ports. For details, see Configuring Security Group Rules.
- Configure local IP addresses, disable external access, disable the UDP protocol, and enable login authentication.
- Adjust some parameters and restart the server to disable UDP.
- Create a profile of normal packet sizes based historical data, so you can easily detect overly small or overly large packets that may be part of the attack traffic.

5 Host Security Checks

5.1 Hosts Security Issues

5.1.1 Overview

Data and programs on servers without protection will probably be breached or tampered with if the servers are intruded, interrupting your business and causing great loss.

This document describes how to defend against the following threats to host security:

- External attacks: port scan
- Mining
- Ransomware

5.1.2 External Attacks: Port Scan

What Is Port Scan?

In a port scan attack, an attacker sends a request to the IP address of a target server or workstation to discover open ports, and exploit vulnerabilities through the port to launch attacks.

Cases

The following are several cases of port scan attacks on hosts:

- Case 1:
 - a. The host is scanning a large number of external ports 6379, as shown in **Figure 5-1**.

Figure 5-1 Port scan

[root[ecs	.2 "]# net	tstat			
Activ	e Interne	t connect	ions (w/o serv	ers)		
Proto	Recv-Q S	end-Q Loca	al Address	Foreig	n Address	State
tcp	0	1 kafl	ka01:34934	1;	6:6379	SYN_SENT
tcp	0	1 kafl	ka01:47186	1:	45:6379	SYN_SENT
tcp	0	1 kafl	ka01:56582	1:	16:6379	SYN_SENT
tcp	0	1 kafl	ka01:55246	1;	11:6379	SYN_SENT
tcp	0	1 kafl	ka01:54150	1:	1:6379	SYN_SENT
tcp	0	1 kafl	ka01:36210	1:	1:6379	SYN_SENT
tcp	0	1 kafl	ka01:51348	1:	7:6379	SYN_SENT
tcp	Ø	1 kafl	ka01:40172	1:	21:6379	SYN_SENT
tcp	0	1 kafl	ka01:35938	1:	39:6379	SYN_SENT
tcp	0	1 kafl	ka01:54252	11	4:6379	SYN_SENT
tcp	0	1 kafl	ka01:43734	1:	17:6379	SYN_SENT
tcp	0	1 kafl	ka01:36836	1:	34:6379	SYN_SENT
tcp	0	1 kafl	ka01:57958	1:	36:6379	SYN_SENT
tcp	0	1 kafl	ka01:57958	1:	5:6379	SYN_SENT
tcp	0	1 kafl	ka@1:53292	1:	48:6379	SYN_SENT
tcp	0	1 kafl	ka01:51384	1:	61:6379	SYN_SENT
tcp	0	1 kafl	ka01:56862	1:	26:6379	SYN_SENT
tcp	0	1 kafl	ka01:53856	1:	:6379	SYN_SENT
tcp	0	1 kafl	ka01:57512	1:	31:6379	SYN_SENT
tcp	0	1 kafl	ka01:55324	1:	43:6379	SYN_SENT
tcp	0	1 kafl	ka01:48428	1:	90:6379	SYN_SENT
tcp	0	1 kafl	ka01:41912	1:	11:6379	SYN_SENT
tcp	0	1 kafl	ka01:43682	1:	60:6379	SYN_SENT
tcp	0	1 kafl	ka01:47736	1:	03:6379	SYN_SENT
tcp	0	1 kafl	ka@1:kitim	1:	7:6379	SYN_SENT
tcp	0	1 kafl	ka01:47290	1:	6:6379	SYN_SENT

- b. The query result shows that these IP addresses are from different countries/regions.
- Case 2:
 - a. An abnormal process is detected on the host, as shown in **Figure 5-2**.

Figure 5-2 Abnormal process

0	0 0.0	.0.0	:13562	0.0.0.0:+	÷	LISTEN	28073/ java
0	0.0	.0.0:	:2181	0.0.0.0:→	÷	LISTEN	27514⁄ java
0	0 1I		93:4181	10	.7:36524	ESTABL ISHED	27514⁄java
0	01		93:8042	10	1:58934	TIME_WAIT	-
0	01		93:48110	10	.7:7184	ESTABL ISHED	27514⁄java
0	0 1I		93:48128	10	7:7184	ESTABL ISHED	27515⁄java
0	01		93:45182	10	7:7182	ESTABL ISHED	24954/python2
0	01		93:52760	21	0:81	ESTABL ISHED	9487/Sof ia
0	01		93:22	11	.233:7847	ESTABL ISHED	10718/sshd: root@pt
0	01		93:2181	16	17:50034	TIME_WAIT	-
0	01		93:9010	10	17:49586	ESTABL ISHED	27514⁄java
0	01		93:39552	10	2.111:10180	ESTABL ISHED	8134/hostguard
0	01		93:41288	10	74:3181	ESTABL ISHED	27514⁄java
0	01		93:34736	16	17:9995	ESTABL ISHED	24954/python2
0	01		93:51410	10	17:8031	ESTABL ISHED	28073/java
0	01		93:9864	16	3:50596	TIME_WAIT	-
0	01		93:9866	16	17:57468	TIME_WAIT	-
0	01		93:22	11	.233:7846	ESTABL ISHED	338/sshd: root@pts/
0	01		93:47758	10	17:9997	ESTABL ISHED	24954/python2
0	01		93:9010	16	17:49592	ESTABL ISHED	27514/java
0	01		1:19001	12	:36230	ESTABL ISHED	24953/python2
0	0 1I		93:4181	16	74:37818	ESTABL ISHED	27514/java
0	01		93:9010	16	17:49562	ESTABL ISHED	27514⁄java
0	01		1:33364	12	:40174	TIME_WAIT	-
0	01		1:36230	12	:19001	ESTABL ISHED	24954/python2
0	0 1L.		93:50046	16	17:8022	ESTABL ISHED	27515/java
Й	й :::	9200		::: *		LISTEN	30648/ java

b. The query result shows that the IP address connects to C&C.
 C&C refers to command and control, a communication mode between hosts.

A C&C host sends commands to a victim system and receives data from the system.

5.1.3 Mining

What Is Mining?

Digital currency, which is decentralized and valuable, is getting more attention nowadays. Black and gray markets obtain digital currency through malicious mining.

Mining is a process of occupying victims' system and network resources and obtaining digital currency through a large amount of computing without permissions.

The machines that can be remotely controlled by attackers are called zombies, which can be the Windows, Linux, or Unix servers of companies, schools, or even governments and militaries.

Mining occupies a large number of system resources and leads to performance deterioration of other software or services. In addition, hackers may use mining programs to obtain confidential information, such as confidential files and the usernames and passwords of key assets.

Cases

The following are several cases of mining:

- Case 1:
 - a. An abnormal file (usually marked with **xmr** or **mine**) is detected.

[root@hecs		7.0	config]#]	ll -art				
total 13676	;						i i	
-rwxrwxrwx	1	oracle	oinstall	54	Jan	9	200 <mark>2</mark>	start
-rwxrwxrwx	1	oracle	oinstall	838583	Jun	15	2018	h64
-rwxr-xr-x	1	oracle	oinstall	337	Feb	14	2020	go
-rwxxx	1	oracle	oinstall	215960	Dec	19	2020	arm
-rwxxx	1	oracle	oinstall	5092504	Dec	19	2020	xmrigMiner
-rwxr-xr-x	1	oracle	oinstall	7805520	Apr	28	13:30	logind
-rwxrwxrwx	1	oracle	oinstall	243	Apr	28	13:3	update
drwxr-xr-x	2	oracle	oinstall	4096	Jun	25	00:25	
-rwxrwxrwx	1	oracle	oinstall	392	Jun	25	00:3 <mark>:</mark>	libs
-rw-rr	1	oracle	oinstall	21	Jun	27	11:59	dir.dir
-rw-rr	1	oracle	oinstall	51	Jun	27	11:59	cron.d
-rwxrr	1	oracle	oinstall	212	Jun	27	11:59	upd
-rwxr-xr-x	1	oracle	oinstall	6	Jun	27	11:59	bash.pid
-rw-rr	1	oracle	oinstall	2771	Jun	27	11:59	config.json
drwx	5	oracle	oinstall	4096	Jun	28	16:44	
[root@hecs-		7.0	config]# p	bwd				
/home/oracl	.e/	.config	7					

- b. Analyze the file. A mining pool is detected. Verify that the URL is a malicious mining pool address.
- Case 2:

- a. A mining process is detected from a Windows host.
- b. Abnormal files are detected from the host.
- c. Analyze the file. A mining pool is detected.



d. Verify that the URL is a malicious mining pool address.

5.1.4 Ransomware

What Is Ransomware?

Ransomware emerged with the Bitcoin economy. It is a Trojan that is disguised as a legitimate email attachment or bundled software and tricks you into opening or installing it. It can also arrive on your servers through website or server intrusion. Ransomware often uses a range of algorithms to encrypt the victim's files and demand a ransom payment to get the decryption key. Digital currencies such as Bitcoin are typically used for the ransoms, making tracing and prosecuting the attackers difficult.

Ransomware interrupts businesses and can cause serious economic losses. We need to know how it works and how we can prevent it.

Ransomware can intrude servers in various ways and is difficult to remove.

Cases

The following are several cases of ransomware:

- Case 1: Files in a Windows host are encrypted and ransomware messages exist in the host.
- Case 2: Files in a Windows host are encrypted and suffixes are added to the files.
- Case 3: Files in a Linux host are encrypted and suffixes are added to the files.

-ru-rr 1	rt	ot	e	37568	Har	28	14:58	/sygroot/bin/sum, locked
-ru-r 1		ot.	Ø	29136	Mar	85	11:58	/sysroot/bin/sync.locked
-ru-rr 1		ot	8	67488	Mar	28	14:58	/sysroot/bin/systemd-hadb.locked
-ru-rr 1	rt	ot	e	53544	Mar	28	14:50	/sysroot/bin/systemd-path.locked
-ru-r 1	-	iot.	я	33392	Mar	28	11:58	/sysroot/bin/tac.locked
-ru-rr 1		ot	0	1781867	Mar	28	14:58	/susroot/bin/tar.locked
-ru-rr 1	r	ot	Ū.	158936	Mar	28	14:58	/sysroot/bin/teamd.locked
-ru-r 1	P1	ot.	R	38616	Mar	28	14:58	/sysroot/bin/testgdbm.locked
-ru-rr 1		ot	0	65928	Mar	28	14:58	/sysroot/bin/tic.locked
-ru-rr 1	r	ot	E.	62616	Mar	28	14:58	/sysroot/bin/touch.locked
-ru-rr 1	Pf	not	e l	15536	Mar	28	14:58	/sysroot/him/tracepath.locked
-ru-rr 1		ot	0	424344	Mar	28	14:58	/sysroot/bin/udevadm.locked
-ru-rr 1	r.	ot	ø	33366	Mar	28	14:58	/sysroot/bin/unexpand.locked
-ru-rr 1	P	not	e	185648	Mar	28	14:58	/sysroot/bin/unzip.locked
-ru-rr 1	E.	ot	0	15984	Mar	28	14:58	/sysroot/bin/usx2yloader.locked
-ru-rr 1	r.	ot	8	1906386	Mar	28	14:58	/sysroot/bin/vim.locked
-ru-rr 1	rt	ot	e	15872	Mar	28	14:58	/sysroot/bin/vxloader.locked
-ru-r 1		ot	ø	156	Mar	28	11:58	/sysroot/bin/wait.locked
-ru-rr 1	r.	\mathbf{ot}	9	24848	Mar	28	14:50	/sysroot/bin/watch.locked
-ru-rr 1	rt	ot	e	41776	Mar	28	14:58	/sysroot/bin/wc.locked
-ru-r 1	P1	10t	а	24464	Mar	28	11:58	/sysroot/bin/which.locked
-ru-rr 1	FC.	\mathbf{ot}	0	2016693	Mar	28	14:58	/sysroot/bin/x86_64-redhat-linux-gcc.locked
-ru-rr 1	PC.	ot	E	9248	Mar	28	14:58	/sysroot/bln/xjc.locked
-ru-rr 1	P	ort.	B	15888	Mar	28	14:58	/sysroot/hin/xmlcataiog.locked
-ru-rr 1		ot	0	24288	Har	28	14:58	/sysroot/bin/xsltproc.locked
-FM-F 1	PO	ot	E	11688	Mar	28	14:58	<pre>/suspoot/bin/ocdec.locked</pre>

5.2 Host Security Check (Windows)

5.2.1 Troubleshooting Methods

You can check Windows hosts by using the methods described below. **Method 1:** Using Tools to Detect Security Issues is recommended.

- Method 1: Method 1: Using Tools to Detect Security Issues (recommended)
- You are advised to use the following software.

Tool	Link
ProcessExplorer	https://learn.microsoft.com/en-us/sysinternals/ downloads/process-explorer
Tcpview	https://docs.microsoft.com/en-us/sysinternals/ downloads/tcpview
Autoruns	https://docs.microsoft.com/en-us/sysinternals/ downloads/autoruns
busybox-x86_64	https://busybox.net/downloads/binaries/1.16.1/ busybox-x86_64

Table 5-1 Software

• Method 2: Method 2: Using DOS System Commands to Check Processes

5.2.2 Troubleshooting Process

5.2.2.1 Method 1: Using Tools to Detect Security Issues

5.2.2.1.1 Step 1: Analyzing All Processes

This section describes how to detect Trojans from official Windows processes.

Prerequisites

You have downloaded Process Explorer.

Procedure

Step 1 Open the ProcessExplorer folder and double-click the procexp64.exe file.

Figure 5-3 processExplorer



Step 2 In the dialog box that is displayed, click **Agree** to view the process information and check the processes online.

5	5		•				
🍣 Process Explorer - Sysinte	ernals:	www.sysinte	ernals.com [HECS-X-MEDIUM-2\Admi	nistrator] (A 🗖 🗖	-	
File Options View Process	Find I	Users Help					
	*	•					
Process	CHO	Frivate B	Working Set	PID Description	Company Name		^
System Idle Process	90.97	1. K	4 K	0			
🖃 🔝 System	0.04	108 K	336 K	4			
Interrupts	0.61	K	K	n/a Hardware Interrupts a			
smss. exe		272 K	1,024 K	192 Windows	Microsoft Corporation		
CSrss. exe	< 0.01	1,944 K	9,788 K	288 Client Server Runtime	Microsoft Corporation		
CSrss. exe	< 0.01	1,364 K	3, 932 К	340 Client Server Runtime	Microsoft Corporation		
wininit.exe		848 K	4,416 K	348 Windows	Microsoft Corporation		
= services. exe	0.01	2,636 K	6,424 K	436	Microsoft Corporation		
svchost. exe		4,224 K	11,964 K	500 Windows	Microsoft Corporation		=
ChsIME. exe	1	1,192 K	5,828 K	236 Microsoft IME	Microsoft Corporation		-
WmiPrvSE. exe		5,880 K	11,616 K	1132 WMI Provider Host	Microsoft Corporation		
ChsIME. exe		1,380 K	6,312 K	2712 Microsoft IME	Microsoft Corporation		
🖃 🚞 explorer. exe	0.02	34, 504 K	60,736 K	1844 Windows	Microsoft Corporation		
💓 procexp64. exe	2.06	18,028 K	32,148 K	2972 Sysinternals Process	Sysinternals - www		
WmiPrvSE. exe		1,828 K	6,292 K	2996 WMI Provider Host	Microsoft Corporation		
svchost. exe	< 0.01	3,476 K	8,172 K	528 Windows	Microsoft Corporation		
svchost. exe	< 0.01	11,928 K	14,640 K	652 Windows	Microsoft Corporation		
svchost. exe		37,168 K	36,724 K	684 Windows	Microsoft Corporation		-
taskhostex. exe		3,660 K	10,884 K	2756 Windows	Microsoft Corporation		
svchost. exe		6,096 K	13,524 K	744 Windows	Microsoft Corporation		
svchost. exe		9,912 K	20,604 K	844 Windows	Microsoft Corporation		
svchost. exe		7,480 K	11,972 K	992 Windows	Microsoft Corporation		
🚔 spoolsv. exe		3,776 К	10,060 K	860	Microsoft Corporation		
wrapper. exe	0.04	2,336 K	7,308 K	1200 Java Service Wrapper	Tanuki Software, Ltd.		
conhost. exe	< 0.01	936 K	4, 284 K	1232	Microsoft Corporation		
🏚 java. exe	0.04	62,340 K	54,004 K	1560 OpenJDK Platform binary	N/A		
svchost. exe		2,524 K	7,752 K	1248 Windows	Microsoft Corporation		
IPROSetMonitor.exe		1,176 K	5,644 K	1412 Intel® PROSet Monitor	Intel Corporation		
dllhost. exe		1,396 K	6,152 K	1508 COM Surrogate	Microsoft Corporation		
svchost. exe		7,928 K	13, 344 K	1552 Windows	Microsoft Corporation		Y

Figure 5-4 Viewing the current process

CPU Usage: 9.03% Commit Charge: 42.90% Processes: 46 Physical Usage: 46.30%

Step 3 On the menu bar, choose Options > VirusTotal.com, and select Check VirusTotal.com and Submit Unknown Executables.

File	Options View Process Find Users	Help		,,	
	Run At Logon				
Proce	Verify Image Signatures	 x	Working Set	PID Description	Company Name
=	VirusTotal.com	•	Check VirusTo	tal.com	
	Always On Top		Submit Unkno	wn Executables	A Microsoft Corp
	Replace Task Manager	8 K	5, 244 K	348 Client Server Run	time Microsoft Corp
=	Hide When Minimized		4,464 K	412 Windows	Microsoft Corp
-	Allow Only One Instance	6 K 6 K	8,112 K 11,740 K	508 596 Windows	Microsoft Corp Microsoft Corp

Figure 5-5 options > VirusTotal.com

The system compares the hash values of the current processes with that in the **VirusTotal** database to quickly detect Trojans.

2		Process	Explorer - S	Sysinternals: www.sysinterr	nals.com [HECS-X-N	/EDIUM-2\/
File Options View Process	Find	Users Help				
۰ ۲۰ ۲۰ 🗖 🔳 🔜 ا	x #	0	~~A			
Process	CPO	Frivate B	Working Set	PID Description	Company Name	VirusTotal
System Idle Process	94. 37	K	4 K	0		
🖃 🔝 System	0.04	108 K	336 K	4		
Interrupts	0.43	K	K	n/a Hardware Interrupts a		
smss. exe		272 K	1,024 K	192 Windows	Microsoft Corporation	<u>0/71</u>
CSTSS. exe	< 0.01	1,944 K	9,788 K	288 Client Server Runtime	Microsoft Corporation	0/72
CSTSS. exe	< 0.01	1,364 K	3,932 K	340 Client Server Runtime	Microsoft Corporation	0/72
🖃 📰 wininit. exe		848 K	4, 416 K	348 Windows /	Microsoft Corporation	0/71
🖃 📰 services. exe		2,620 K	6,380 K	436	Microsoft Corporation	0/72
🖃 💼 svchost. exe		4 , 212 K	11, 936 K	500 Windows	Microsoft Corporation	<u>0/71</u>
ChsIME. exe		1,192 K	5,828 K	236 Microsoft IME	Microsoft Corporation	0/68
WmiPrvSE. exe	1.03	5, 884 K	11,624 K	1132 WMI Provider Host	Microsoft Corporation	0/71
ChsIME. exe		1,380 K	6,312 K	2712 Microsoft IME	Microsoft Corporation	0/68
🖃 🚞 explorer. exe		34, 044 K	60,436 K	1844 Windows	Microsoft Corporation	0/70
🖉 procexp64. exe	0.64	20, 288 K	39, 212 K	2972 Sysinternals Process	Sysinternals - www	0/72
WmiPrvSE. exe		1,644 K	6,224 K	2996 WMI Provider Host	Microsoft Corporation	0/71
svchost. exe	0.03	3,420 K	8,152 K	528 Windows	Microsoft Corporation	0/71
svchost. exe	0.04	12,016 K	14,704 K	652 Windows	Microsoft Corporation	0/71
🖃 📑 svchost. exe	0.49	36, 992 K	36,756 K	684 Windows	Microsoft Corporation	0/71
taskhostex. exe		10,052 K	17,780 K	2756 Windows	Microsoft Corporation	0/72
svchost. exe		6,204 K	13,848 K	744 Windows	Microsoft Corporation	0/71
svchost. exe		10,648 K	21, 136 K	844 Windows	Microsoft Corporation	0/71
svchost. exe		7,572 K	12,056 K	992 Windows	Microsoft Corporation	0/71
🚔 spoolsv. exe		З, 776 К	10,060 K	860	Microsoft Corporation	0/72
- 🚳 wrapper. exe	0.04	2,336 K	7,308 K	1200 Java Service Wrapper	Tanuki Software, Ltd.	3/72
conhost. exe	< 0.01	936 K	4,284 K	1232	Microsoft Corporation	0/72
java. exe	0.04	62,340 K	54,004 K	1560 OpenJDK Platform binary	N/A	0/76
svchost. exe		2, 524 K	7,752 K	1248 Windows	Microsoft Corporation	0/71
IPROSetMonitor.exe		1,176 K	5,644 K	1412 Intel® PROSet Monitor	Intel Corporation	0/72
dllhost.exe	< 0.01	1,396 K	6,152 K	1508 COM Surrogate	Microsoft Corporation	0/72
svchost. exe		7,928 K	13, 344 K	1552 Windows	Microsoft Corporation	0/71
vm-agent-daemon. exe		788 K	3,744 K	1592		2/72
dllhost.exe	< 0.01	3, 304 K	11, 224 K	2160 COM Surrogate	Microsoft Corporation	0/72
= svchost. exe	0.63	70, 760 K	87, 376 K	2240 Windows	Microsoft Corporation	0/71
rdpclip. exe	< 0.01	2, 440 K	9,852 K	2116 RDP	Microsoft Corporation	0/72
and and and		1 070 4	E 004 W	0000 mi - 1	11	0/71

Figure 5-6 Process Explore-Sysinternals

Step 4 Check the value of **VirusTotal**. Right-click a process name and choose **Properties** from the shortcut menu. On the page that is displayed, click **Image** from the menu bar to view the process path and determine whether the process is a Trojan.

Figure 5-7 Checking whether a program is a Trojan horse program

hgdpnm.exe:3800 Properties	X IFOCESS FI	nd Osers neip				
Services Threads TCP/IP Security Environment Strings	📑 🙆 🔗	Х М 🚯 📃				A
Image Performance Performance Graph Disk and Network		CPU Private B	Working Set	PID Description	Company Name	VirusTotal
	e	3, 232 K	5,780 K	2188	Microsoft Corporation	0/56
Image File	eze	< 0.01 24,440 K	29, 980 K	556 Windows	Microsoft Corporation	0/55
	p. eze	4, 700 X	10,492 K	2100 RDP Clip	Microsoft Corporation	0/55
	0IR	7, 728 K	13,204 K	1095 Windows	Microsoft Corporation	0/55
	eze	< 0.01 8,696 K	15,740 K	1308 /	Microsoft Corporation	0/56
Version: n/a	eze	6,452 X	11,664 K	1348 Windows /*******	Microsoft Corporation	0/55
Build Time: Thu May 28 03:29:13 2015	eze	13,895 X	22, 072 K	1392 Internet Information	Microsoft Corporation	0/57
Path (Image is probably packed):	ez e	2, 928 X	6,928 K	1532 Windows	Microsoft Corporation	0/55
Cultific deputition depute	leService. eze	2, 980 K	5,408 K	1640		Unknown
C://windows/rigdpinin.exe	pr. eze	< 0.01 7,056 K	9,600 K	1700		Unknown
Command line:	ez e	1,484 X	3, 532 K	1716 Windows	Microsoft Corporation	0/55
C:\Windows\hgdpmm.exe	ez e	2, 580 X	8, 596 K	2740 Windows	Microsoft Corporation	0/55
Current directory:		4, 092 K	8,836 K	2776 MS DTCconsole	Microsoft Corporation	0/57
	PZP.	4, 408 K	6,404 K	2180 Windows	Microsoft Corporation	0/55
C:(Windows(5)/stem32)	7	< 0.01 3,012 X	6,732 K	3800		40/56
Autostart Location:		< U. U1 9, 444 K	15, 980 K	640	Alcrosoft Corporation	0/55
n/a Explore		6, 716 X	9, 844 K	648	Microsoft Corporation	0/55
		< 0.01 2,295 K	6,252 K	552	Microsoft Corporation	0/55
Parent: services.exe(628)		2, 192 K	5,808 K	596 Windows	Microsoft Corporation	0/57
I CERT NT ALITHORITY/SYSTEM		< 0.01 9,604 X	15,352 K	928 Windows Logon User In	Microsoft Corporation	0/57
Bring to Front		< 0.01 4,440 K	18,444 K	960	Microsoft Corporation	0/55
Started: 16:49:11 2015/8/18 Image: 32-bit		2, 900 K	6,972 K	1808 Windows	Microsoft Corporation	0/57
Kill Process		< 0.01 37, 340 K	55,732 K	2224 Windows	Microsoft Corporation	0/57
	e. eze	< 0.01 1,704 K	5,148 K	2340		Unknown
virusTotal: 40/56 Submit		4, 508 X	8,136 K	3764 Sysinternals Process	. Sysinternals - www	0/56
	. eze	< 0.01 22,724 K	33, 428 K	995 Sysinternals Process	. Sysinternals - www	0/56
	er. eze	12, 120 K	22,128 K	256 Windows	Microsoft Corporation	0/57
Address Space Load Randomization: Disabled		0.39 6,524 K	12,712 K	3748 TCP/UDP endpoint viewer	Sysinternals - www	0/56
		< 0.01 2,984 K	9, 208 K	1384 Windows	Microsoft Corporation	0/57

----End

5.2.2.1.2 Step 2: Detecting Automatic Startup Programs

This section describes how to use **Autoruns** to check which programs are configured to automatically start upon system startup and login.

Prerequisites

You have downloaded Autoruns.

Procedure

Step 1 Open the Autoruns folder and double-click the Autoruns.exe file.

Figure 5-8 Opening the AutoRuns folder



Step 2 In the displayed dialog box, click Agree.

Figure 5-9 AutoRuns

Autoruns (HEC)	CS-X-MEDIUM-2\/	dministrato] - Sysinterna	ls: www.sysi	internals.com	
File Entry Options User Help						
🖬 🖬 🏔 🗶 🦉 Filter:						
😭 Winlogon 🚯 Winsock Providers	Print Monitors	🕴 LS/	A Providers	2	Network Providers	🗐 WMI
🖉 Everything 🏼 😹 Logon 🛛 🚼 Explorer 🛛 🙆 Internet Explorer	🕙 Scheduled Tasks	📓 Drivers	Codecs	Boot Execute	📑 Image Hijacks	
Autorun Entry Description Publisher	Timestamp	Virus	otal			
HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup				2019/4/11 1	5:37	
	c:\program files (x86)\virti	o\bin\install_viosto	or.bat	2019/5/8 10	05	
HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown				2019/4/11 1	5:37	
	File not found: c:\uvptool	s_temp\pvdriver\s	hutdown.bat			
	File not found: c:\uvptool	s_temp\inic\shutd	own.bat			
	File not found: c:\uvptool	s_temp\vda\shutd	own.bat			
	File not found: c:\vmtools	upgrade\vmtools	shutdown.bat			
	File not found: C:\vmtools	_upgrade\vmtools	\shutdown.bat			
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2013/8/22 2	2:48	
Contraction of the second seco	c:\windows\system32\cn	nd.exe		2014/10/29	9:28	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\Avai	lableShells			2013/8/22 2	3:40	
30000	File not found: cd /d					
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2019/8/15 1	5:34	
M HWUVPUPGR Huawei Upgrade Tray	c:\program files (x86)\xer	pv drivers\bin\hw	uvpupgrade.exe	2019/8/1 18	49	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2019/8/15 2	0:02	
🗹 🕅 HwUVPUpgrade Huawei Upgrade Tray	c:\program files (x86)\xer	pv drivers\bin\hw	uvpupgrade.exe	2019/8/1 18	49	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020/6/28 9	:55	
Microsoft Windo	File not found: C:\Program	n Files\Windows M	lail\WinMail.exe			
Microsoft .NET IE SECURIT (Verified) Microsoft Corporation	c:\windows\system32\m	cories.dll		2013/8/14 1	2:56	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020/6/28 9	55	
Microsoft Windo	File not found: C:\Program	n Files\Windows M	ail\WinMail.exe			
Microsoft .NET IE SECURIT (Verified) Microsoft Corporation	c:\windows\syswow64\n	iscories.dll		2013/8/14 1	3:35	
Task Scheduler						
🗹 📰 \Microsoft\Win Microsoft Windows Diagnosti (Verified) Microsoft Corporation	c:\windows\system32\co	mpattel\diagtrackr	unner.exe	2015/11/10	11:58	
Microsoft Win Microsoft Compatibility Telem (Verified) Microsoft Corporation	c:\windows\system32\cc	mpattelrunner.exe		1941/5/27 1	4:26	
Microsoft Win Microsoft Compatibility Telem (Verified) Microsoft Compration	c./windowe/eveterm 32/co	mnatteln inner eve		1941/5/27 1	4-26	

Step 3 On the menu bar, choose Options > Scan Options and select CheckVirusTotal.com to enable the online process detection function.

File Entry Option	ons User He	elp	
🐱 🗈 🗚 🕗 🕽	< Ķ 🛛 Filte	r:	
🔇 Winso	ck Providers	8	Print Monitors
C Everything	🖽 Logon	🛃 Explorer	🥭 Internet Explorer
Autorun Entry HKLM\SOFTW AdobeA Memory BLESen Memory BTMTra	Autoruns Scan	Options er-user locations signatures	x)
 Enhance HotKeys IgfxTray 	Check Virus	Total.com Inknown Images	
Persister SynTPB		Resca	an Cancel

Step 4 Check whether abnormal files (not created for system or normal service deployment) exist in the **Autorun** and **Images Path** columns.

J		Autoruns [HE	CS-X-MEDIUM-2	\Administrator] ·	- Sysinternals	s: www.sy	sinternals.com			_ 0 X
File Entry Options U	Jser Help									
	Filter:									
😫 Winlogon	🔌 Winsock Pr	roviders	Print Monitors	💔 LSA Pi	oviders	ĝ	Network Providers	🗃 wmi		1 Office
🖾 Everything 🛛 🆽	Logon 🚼 Explorer	Internet Explorer	🙆 Scheduled Tasks	Services	B Drivers	Codecs	Boot Execute	📑 Image Hijacks	AppInit	S KnownDLLs
Autorun Entry	Description	Publisher	Image Path			Timestamp	VirusT	otal		
🗹 🚳 n/a	Microsoft .NET IE SECURIT	(Verfied) Microsoft Corporatio	n c:\windows\system32\	mscories.dl		2013/8/14	12:56			
HKLM\SOFTWARE\W	w6432Node\Microsoft\Active S	Setup \Installed Components				2020/6/28	9:55			
Microsoft Windo.			File not found: C:\Progr	ram Files\Windows Mail\	WinMail.exe					
🗹 🚳 n/a	Microsoft .NET IE SECURIT	. (Verified) Microsoft Corporatio	n c:\windows\syswow64	Vmscories.dll		2013/8/14	13:35			
Task Scheduler										
✓ III \Microsoft\Win	Microsoft Windows Diagnosti.	(Verfied) Microsoft Corporatio	n c:\windows\system32\	compattel\diagtrackrunn	ner.exe	2015/11/10	11:58			
✓ III \Microsoft\Win	Microsoft Compatibility Telem.	(Verfied) Microsoft Corporatio	n c:\windows\system32\compattelrunner.exe			1941/5/27	14:26			
✓ III \Microsoft\Win	Microsoft Compatibility Telem.	(Verfied) Microsoft Corporatio	n c:\windows\system32\compattelrunner.exe			1941/5/27	14:26			
HKLM\System\CurrentC	ontrolSet\Services					2022/3/24	3:05			
 cloudbase-init 	cloudbase-init: Cloud Initializ	. (Not verified) Cloudbase Solu	c:\program files\cloudb	base solutions/cloudbase	e-init/bin/opensta	2015/5/12	21:45			
✓ I cloudResetPwd.	. cloud reset password agent: .	(Verfied) Tanuki Software Ltd	 c:\cloudresetpwdagent 	t\bin\wrapper.exe		2014/12/5	17:37			
✓	. cloud reset password update.	(Verfied) Tanuki Software Ltd	 c:\cloudresetpwdupdat 	teagent \bin \wrapper.exe		2014/12/5	17:37			
FontCache3.0.0.	Windows Presentation Foun	. (Verified) Microsoft Corporatio	n c:\windows\microsoft.n	net/framework64/v3.0/w	<pre>/presentationfo.</pre>	. 2013/7/20	13:58			
 HostGuard 	HostGuard:	(Verfied) Huawei Technologi.	c:\program files (x86)\h	nostguard/hostguard.exe	5	2020/7/14	10:23			
✓ ■ HostWatch	HostWatch:	(Verfied) Huawei Technologi.	c:\program files (x86)\h	nostguard/hostwatch.exe	•	2020/7/14	10:23			
Intel(R) PROSet.	. Intel(R) PROSet Monitoring	(Not verified) Intel Corporation	c:\windows\system32\	iprosetmonitor.exe		2018/5/3 2	:16			
UVPMonitor	Huawei UVP Monitor Tools:		c:\program files (x86)\x	en pv drivers/bin/uvpm	onitor.exe	2019/8/1 1	8:51			
✓ ■ vm-agent	vm-agent: Enables integratio	. (Not verified) http://www.qe	c:\program files (x86)\v	virtio \monitor \vm-agent.e	xe	2018/12/20	0:00			
VmAgentDaemor	VMTools Daemon Service: V.		c:\program files (x86)\v	virtio \monitor \vm-agent-d	aemon.exe	2019/5/8 1	8:05			
HKLM\System\CurrentC	ontrolSet\Services					2022/3/24	3:05			
HWWebGuard	HWWebGuard: HWWebGu	. (Not verified) Huawei Techn	. c:\windows\system32\	drivers hwwebguard sys	l.	2018/8/13	15:07			
✓ iaStorAV	Intel(R) SATA RAID Controll	(Verfied) Intel Corporation - I.	c:\windows\system32\	drivers \iastorav.sys		2013/8/18	:00			
🗹 🚳 von	Intel(R) 10G Virtual Network	(Verfied) Intel Corporation	c:\windows\system32\	drivers\vxn64x64.sys		2014/3/53	:54			
HKLM\SOFTWARE\Cla	sses \Htmitile \Shell \Open \Comn	nand (Default)				2013/8/22	23:46			
C:\Program File	Internet Explorer	(Ventied) Microsoft Corporatio	n c:\program files\interne	st explorer/vexplore.exe		2018/5/25	11:12			
HKLM\System\CurrentC	ontrolSet (Control\Session Mana	ager \Known Dils				201////51	5:48			

Step 5 If a suspicious process is found, double-click the process name to locate the registry. You can search for the names of suspicious processes in the **Filter** box.

🛃 🕄 👫 🛃 🗙 Ķ Filte	ar: dhep				
🔇 Winsock Providers 🗇 Everything 🛛 🛃 Logon	Series Print Monitor	s t Explorer	💔 LSA P ピ 🕄	roviders asks 🏾 🏶 Services	Vetwork Providers
Autorun Entry HKLM\System\CurrentControlSet\ MyWiFiDHCPDNS Numeric VMnetDHCP	Description Services Wireless PAN DHCP and D	Publisher	k c:	nage Path \program files\intel\wifi\t	sin\pandhcpdns.exe
	usbuhci usbvideo usbvideo UxSms VaultSvc VBoxNetAdp VBoxNetFlt vcsFPService vdvroot vdvroot		DependOnSer Description DisplayName ErrorControl ImagePath ObjectName Start	REG_SZ REG_MULTI_SZ REG_SZ REG_SZ REG_DWORD REG_EXPAND_SZ REG_SZ REG_DWORD	VMnetuserif DHCP service for virtual networ VMware DHCP Service 0x00000001 (1) C:\Windows\system32\vmneto LocalSystem 0x00000002 (2)

Figure 5-10 Opening the Registry Editor

----End

5.2.2.1.3 Step 3: Analyzing the Network

This section describes how to use **TCPView** to view the current TCP connection status and detect suspicious processes. Suspicious processes are highlighted in red.

Prerequisites

You have downloaded the **TCPView** tool.

Procedure

Step 1 Open the **TCPView** folder and double-click the **Tcpview.exe** file. In the displayed dialog box, click **Agree**.

📥 TCPView - S	ysinternals: 🕶	w. sysinternal:	5. COM					_ 🗆 ×
File Options	Process View He	lp						
🖬 A 🛶 😰								
Process A	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Pa
🔟 hgdpmm, eze	3800	TCP	win-5iw7pi37uao	19201	125.77.29.72	7890	ESTABLI SHED	
bgdomm, exe	3800	TCP	win-Siw7pi37uag	19293	125, 77, 29, 72	6666	SYN SENT	
📫 hgdpmm. eze		TCP	win=5iw7pj37uaq	19295	125.77.29.72	6666	SYN SENT	
📑 lsass. eze	640	TCP	WIN-51W7PJ37UAQ	1028	WIN-51W7PJ37UAQ	0	LISTENING	
📑 lsass. eze	640	TCPV6	win-5iw7pj37uaq	1028	win-5iw7pj37uaq	0	LISTENING	
🛒 services, eze	628	TCP	WIN-51W7PJ37UAQ	1029	WIN-51W7PJ37UAQ	0	LISTENING	
🛒 services, eze	628	TCPV6	win-5iw7pj37uaq	1029	win-5iw7pj37uaq	0	LISTENING	
🛒 svchost, eze	860	TCP	WIN-51W7PJ37UAQ	epmap	WIN-51W7PJ37UAQ	0	LISTENING	
🛒 svchost, eze	936	TCP	WIN-51W7PJ37UAQ	1026	WIN-51W7PJ37UAQ	0	LISTENING	
🗐 svchost. eze	1016	TCP	WIN-51W7PJ37UAQ	1027	WIN-51W7PJ37UAQ	0	LISTENING	
🗐 svchost. eze	556	TCP	WIN-51W7PJ37UAQ	ms-wbt-server	WIN-51W7PJ37UAQ	0	LISTENING	
🗐 svchost. eze	556	TCP	win-5iw7pj37uaq	ms-wbt-server	223. 202. 3. 14	26993	ESTABLI SHED	
🗐 svchost. eze	344	VDP	WIN-51W7PJ37UAQ	ntp	*	*		
🗐 svchost. eze	1016	VDP	WIN-51W7PJ37UAQ	i sakmp	*	*		
🗐 svchost. eze	1016	VDP	WIN-51W7PJ37UAQ	ipsec-msft	*	*		
🔟 svchost, eze	556	UDP	WIN-51W7PJ37UAQ	llmnr	*	*		
🛒 svchost, eze	860	TCPV6	win-5iw7pj37uaq	epmap	win-5iw7pj37uaq	0	LISTENING	
🛒 svchost, eze	936	TCPV6	win-5iw7pj37uaq	1026	win-5iw7pj37uaq	0	LISTENING	
🎫 svchost. eze	1016	TCPV6	win-5iw7pj37uaq	1027	win-5iw7pj37uaq	0	LISTENING	
🗐 svchost, eze	556	TCPV6	win-5iw7pj37uaq	ms-wbt-server	win-5iw7pj37uaq	0	LISTENING	
🛒 svchost, eze	344	UDPV6	win-5iw7pj37uaq	123	*	*		
🛒 svchost, eze	1016	UDPV6	win-5iw7pj37uaq	500	*	*		
🗐 svchost. eze	556	VDPV6	win-5iw7pj37uaq	5355	*	*		
🗐 svchost. eze	936	VDPV6	win-5iw7pj37uaq	546	*	*		
📑 System	4	TCP	win-5iw7pj37uaq	netbios-ssn	WIN-51W7PJ37UAQ	0	LISTENING	
System	4	TCP	WIN-51W7PJ37UAQ	microsoft-ds	WIN-51W7PJ37UAQ	0	LISTENING	
System	4	TCP	WIN-51W7PJ37UAQ	47001	WIN-51W7PJ37UAQ	0	LISTENING	
📑 System	4	UDP	win-5iw7pj37uaq	netbios-ns	*	*		
📑 System	4	UDP	win-5iw7pj37uaq	netbios-dgm	*	*		
📑 System	4	TCPV6	win-5iw7pj37uaq	microsoft-ds	win-5iw7pj37uaq	0	LISTENING	_
📑 System	4	TCPV6	win-5iw7pj37uaq	47001	win-5iw7pj37uaq	0	LISTENING	
84 System	4	TCP	win-5iw7pj37uag	19279	10, 120, 157, 1	netbios-ssn	SYN SENT	
W/I minimit and	Edd	TCD	DIN-FIDIDI STHAO	1005	MIN-FIRTRI STIMO	0	LICTIVIA	

Step 2 Check the TCP connection status of the target process to analyze whether it is a Trojan.

- If an unknown process has a large number of connections in the **SYN_SENT** state, the process may be a Trojan.
- If a process connects to regular ports (for example, 6666 or 2333), or its host automatically parsed in the **RemoteAddress** column contains keywords such as **mine**, **pool**, or **xmr**, the process may be infected with viruses.

11000033		11010001	BOCGE AGGECOS	20001 1011	nemote Address	ACHIOTE TOTE	Diale .
📰 cwuoky. eze	1620	TCP	192.168.1.40	53318	119, 90, 12, 136	6431	SYN_SENT
💼 cwioky, exe	1620	TCP	192.168.1.40	53319	119.90.12.136	6431	SYN SENT
Cwuoky, exe	1620	TCP	192, 168, 1, 40	53320	119, 90, 12, 136	6431	SYN SENT
Cwioky, eze	1620	TCP	192, 168, 1, 40	53321	119, 90, 12, 136	6431	SYN SENT
Cunicky, exe	1620	TCP	192, 158, 1, 40	53322	119.90.12.135	6431	SYN SENT
CWNOKT, exe	1620	TCP	192, 158, 1, 40	53324	119, 90, 12, 135	6431	SYN SENT
cunicky exe	1620	TCP	192 158 1 40	53326	119 90 12 135	6431	SYN SENT
cunicky exe	1520	TCP	192 158 1 40	53327	119 90 12 136	6431	SYN SENT
 cynoky, eze 							
cunicky exe		TCP	192 168 1 40	53329	119 90 12 135	6431	SYN SENT
cunoky exe	1620	TCP	192 158 1 40	53330	119 90 12 135	6431	SYN SENT
cunicky eye	1620	TCP	192 158 1 40	53331	119 90 12 135	6431	SYN SENT
cunicky exe	1620	TCP	192 158 1 40	53332	119 90 12 135	6431	SYN SENT
cunicky exe	1620	TCP	192 158 1 40	53333	119 90 12 136	6431	SYN SENT
cunicky eye	1620	TCP	192 158 1 40	53334	119 90 12 135	6431	SYN SENT
cunicky exe	1620	TCP	192 168 1 40	53335	119 90 12 135	6431	SYN SENT
Cumicky eve	1620	TCP	192 168 1 40	53336	119 90 12 136	6431	SYN SENT
cunicky eye	1620	TCP	192 158 1 40	53337	119 90 12 135	6431	SYN SENT
cunicky exe	1620	TCP	192 168 1 40	53338	119 90 12 135	6431	SYN SENT
Cumoky ere	1620	TCP	192 168 1 40	53339	119 90 12 136	6431	SYN SENT
Cumoky, ere	1520	TCP	192 158 1 40	53340	119 90 12 136	6431	SYN SENT
Cumoky, ere	1620	TCP	192 168 1 40	53341	119 90 12 135	6431	SYN SENT
cumoky, ere	1620	TCP	192 169 1 40	59942	119 90 12 196	6491	CAN CENT
	1620	TCP	192 168 1 40	53343	119 90 12 136	6431	SYN SENT
	1620	TCP	192 168 1 40	533dd	119 90 12 135	6431	SYN SENT
cumoky, ere	1620	TCP	192 169 1 40	59945	119 90 12 196	6491	CAN CENL
Cumoky, ere	1620	TCP	192 158 1 40	53346	119 90 12 136	6431	SYN SENT
	1620	TCP	192 168 1 40	53347	119 90 12 135	5431	SYN SENT
cumoky, ere	1620	TCP	192 169 1 40	52249	119 90 12 195	6491	CVN CENT
	1620	TCP	192 168 1 40	53349	119 90 12 136	6431	SYN SENT
cwabky.exe	1620	TCD	192.100.1.40	52250	119 90 12 195	C/01	CVN CENT
cwabky.exe	1620	TCP	192 169 1 40	59951	119 90 12 196	6491	CAN CENT
cwabky.exe	1620	TCD	192.100.1.40	50050	110 00 12 120	C/01	CVN CENT
cwasky, ere	16.20	TCD	192 169 1 40	52254	110 00 12 126	5491	CAN CENT
CWOOKT. exe	1620	TOP	192 169 1 40	52255	119 90 12 196	6491	CVN CENT
cwasky.exe	1620	TCP	192 169 1 40	53356	119 90 12 135	5431	SYN SENT
cwasky, ere	16.20	TCD	192 100 1 40	52257	110 00 12 120	5491	CAN CENT
cwadky, exe	1620	TOP	192,160,1,40	50050	119 90 12 196	6491	CVN CENT
CwaDky, exe	1020	TOD	102.100.1.40	50050	110.00.12.100	C A DA	CIN CONT

Step 3 (Optional) You can use the security detection websites to check external remote addresses or URLs.

----End

5.2.2.1.4 Step 4: Detecting Abnormal Users

This section describes how to detect abnormal users.

Procedure

Step 1 Choose **Control Panel > Administrative Tools > Computer Management**.

🗄 🗹 📕 🖛 I		Manage	Adminis	trative Tools			- 0	\times
File Home Sh	are View	Shortcut Tools						~
$\leftarrow \rightarrow \cdot \uparrow $	Control Pane	I > All Control Pan	el Items	> Administrative To	ools 🗸 🗸	Sea	rch Administrative Tool	s 🔎
📌 Quick access	Name		^		Date modified		Туре	Size
Desktop	💉 📙 Ter	minal Services			9/15/2018 3:19 PM		File folder	
	🍌 🔔 Co	mponent Services			9/15/2018 3:12 PM		Shortcut	
Downloads	🀊 🛃 Co	mputer Manageme	nt		9/15/2018 3:12 PM		Shortcut	
Documents	🌋 1 👬 De	fragment and Optir sk Cleanup	mize Mar rem	nages disks and pro lote computers.	wides access to other	r tool	s to manage local and	
🧢 This PC	🗿 Eve	ent Viewer			9/15/2018 3:12 PM		Shortcut	
3D Objects	🔧 isc	SI Initiator			9/15/2018 3:12 PM		Shortcut	
	ᡀ Lo	cal Security Policy			9/15/2018 3:13 PM		Shortcut	
	🌮 Mi	crosoft Azure Servic	es		9/15/2018 3:13 PM		Shortcut	
Documents	70 💦	DBC Data Sources (3	2-bit)		9/15/2018 3:12 PM		Shortcut	
👆 Downloads	🔊 OE	DBC Data Sources (6	i4-bit)		9/15/2018 3:12 PM		Shortcut	
👌 Music	🔊 Per	rformance Monitor			9/15/2018 3:12 PM		Shortcut	
Note: Pictures	😺 Pri	nt Management			9/15/2018 3:13 PM		Shortcut	
📑 Videos	🔊 Re	covery Drive			9/15/2018 3:12 PM		Shortcut	
👟 Local Disk (C:)	💏 Re	gistry Editor			9/15/2018 3:12 PM		Shortcut	
	🔊 Re	source Monitor			9/15/2018 3:12 PM		Shortcut	
学 Network	📠 Se	rver Manager			9/15/2018 3:13 PM		Shortcut	
	🛞 Se	rvices			9/15/2018 3:12 PM		Shortcut	
	🔝 Sys	stem Configuration			9/15/2018 3:12 PM		Shortcut	
	😰 Sys	stem Information			9/15/2018 3:13 PM		Shortcut	
	<							>

Step 2 In the navigation pane on the left, choose **Local Users and Groups** > **Users** to check whether abnormal users exist in the host.

🛃 Computer Management					-	Х
File Action View Help						
🗢 🄿 🙋 🖬 🙆 🖬 🚺	8					
🛃 Computer Management (Local)	Name	Full Name	Description	Action	ıs	
 V System Tools 	🛃 Administrator		Built-in account for administering the c	Users		
 > Task Scheduler > Event Viewer > Shared Folders > Coal Users and Groups > Operformance Device Manager > Storage > Windows Server Backup > Disk Management > Services and Applications 	y cloudbase-init UpfaultAccount Guest WDAGUtilityAccount	doudbase-init	A user account managed by the system. Built-in account for guest access to the A user account managed and used by t	N	fore Actions	•

Step 3 In the navigation pane on the left, choose **Local Users and Groups** > **Groups** to check whether abnormal groups exist in the host.

le Action view neip			
🔿 🙋 🖬 🙆 🛃			
Computer Management (Local)	Name	Description	Actions
👔 System Tools	🜆 Access Control Assistance Operat	Members of this group can remot	Groups
> 🕑 Task Scheduler	Administrators	Administrators have complete and	More Actions
> 🛃 Event Viewer	🜆 Backup Operators	Backup Operators can override sec	Wore Actions
> 8 Shared Folders	ntificate Service DCOM Access	Members of this group are allowe	
 Local Users and Groups 	ntering the term of te	Members are authorized to perfor	
Groups	A Device Owners	Members of this group can chang	
> Performance	are Distributed COM Users	Members are allowed to launch, ac	
- Device Manager	🜆 Event Log Readers	Members of this group can read e	
Storage	🜆 Guests	Guests have the same access as m	
> 🐌 Windows Server Backup	nter-V Administrators	Members of this group have comp	
📅 Disk Management	📲 IIS_IUSRS	Built-in group used by Internet Inf	
Services and Applications	Network Configuration Operators	Members in this group can have s	
	nerformance Log Users	Members of this group may sched	
	nerformance Monitor Users	Members of this group can access	
	🚈 Power Users	Power Users are included for back	
	🜆 Print Operators	Members can administer printers i	
	🜆 RDS Endpoint Servers	Servers in this group run virtual m	
	🜆 RDS Management Servers	Servers in this group can perform r	
	🜆 RDS Remote Access Servers	Servers in this group enable users	
	🜆 Remote Desktop Users	Members in this group are grante	
	🜆 Remote Management Users	Members of this group can access	
	and Replicator	Supports file replication in a doma	
	🜆 Storage Replica Administrators	Members of this group have comp	
	🌆 System Managed Accounts Group	Members of this group are manag	
	🛃 Users	Users are prevented from making	

Step 4 Check whether abnormal files (not created by the system or service deployment) exist in the abnormal user directory.

	This i e i r cour bisk (e.) i osers i	admin + besitep +		
uick access	Name	Date modified	Туре	Size
Desktop	source.txt	1/10/2021 11:09 PM	Text Document	2,499 KB
Downloads	👔 config.ini	1/10/2021 7:27 PM	Configuration settings	1 KB
owniouds /	good.txt	1/10/2021 7:27 PM	Text Document	1 KB
cuments	ip.txt	1/10/2021 7:24 PM	Text Document	1,096 KB
tures ;	bad.txt	1/10/2021 7:24 PM	Text Document	762 KB
PC	error.txt	1/10/2021 7:24 PM	Text Document	8,698 KB
	crashlog.txt	1/10/2021 2:16 PM	Text Document	15 KB
ork	🗋 dump.dmp	1/10/2021 2:16 PM	DMP File	5,003 KB
	DUB2.1.exe	1/5/2021 2:27 PM	Application	25 KB
	🗟 libeay32.dll	1/5/2021 2:27 PM	Application extension	992 KB
	🗟 msvcr71.dll	1/5/2021 2:27 PM	Application extension	340 KB
	🖲 QtCore4.dll	1/5/2021 2:27 PM	Application extension	1,580 KB
	🗟 QtGui4.dll	1/5/2021 2:27 PM	Application extension	5,464 KB
	🗟 ssleay32.dll	1/5/2021 2:27 PM	Application extension	192 KB
	pass.txt	1/1/2021 11:39 PM	Text Document	1,196 KB
	pass	9/11/2022 10:47 AM	File folder	
	user	9/11/2022 10:46 AM	File folder	
	windowstools	9/11/2022 10:43 AM	File folder	

Step 5 Check whether the abnormal files are used for normal services, or use antivirus software to scan the abnormal files.

			op			 · O Search Desktop
★ Quick access Desktop # ♦ Downhoads # ♦ Downhoads # ♦ Downhoads # ♦ Downhoads # ♦ Network	Name source.bt config.ini good.bt ip.txt bad.bt eror.bt crashlog.bt dump.dmp DU82.2dl msvc71.dl CtCore4.dl CtCore4.dl sslevy2.2dl pass.bt pass.bt user windowstools	pass.bt Notepad File Edit Format View 123 123123 123321 111111 88888 1234567890 1qa2xwsx 123qwe 1qa2xws 123yee 1qa2xws 123qwe 1qa2xws 123456789 12345678 12345678 12344 12345678 1234 12345678 1234 12345678 1234 12345678 1234 12345678 1234 12345678 1234 1234578 1234 123459 12341 123459 12341 123459 123459 123459 123459 123459 123459 123459	Data modified	Tuna	Sim	-
		1399867338200				

----End

5.2.2.2 Method 2: Using DOS System Commands to Check Processes

This section describes how to use DOS commands to check processes.

Common Commands

Command	Description
cd	Switch to the following directory:
	• Current directory: [./] It can be omitted.
	One level up: [/]
	• Two levels up: [//]
dir /a: (disk)	Display all files (including system files and hidden files) by default.
more	Display file contents in the split-screen mode.
tasklist	Check process status.
netstat -ano	View links.
wmic startup list full	View automatic startup programs.
net user	View users.

Example commands are as follows:

- Search for the files that contain DR under the D:\Apps\ directory: dir /a-d /s "D:\Apps\IDE" | findstr "DR"
- Search for the files and directories that contain **exe** in drive C: **dir /s C**: | **findstr "exe"**

Procedure

Step 1 Check whether abnormal processes exist.

Command: tasklist

Based on the query result, locate abnormal processes that are neither system processes nor service application processes.

	14.4.100				
Microsoft Windows [Versic (c) 2018 Microsoft Corpor	n 10.0.177 ation. All	'63.5329J rights reserv	ed.		
C:\Users\Administrator>ta	sklist				
Image Name	PID	Session Name	Session#	Mem Usage	
System Idle Process	0	Services	0 0	8 K	
System	4	Services	Ő	152 K	
Registry	84	Services	Ő	21.588 K	
snss.exe	268	Services	0	1,200 K	
csrss. exe	372	Services		5,612 K	
wininit.exe	448	Services		7,084 K	
CSTSS. exe	456	Console	1	5,316 K	
winlogon. exe	520	Console	1	13,268 K	
services.exe	592	Services		9,744 K	
lsass.exe	600	Services		16,852 K	
svchost.exe	716	Services		4,120 K	
svchost.exe	736	Services		22,488 K	
fontdrvhost.exe	756	Console	1	5,592 K	
fontdrvhost. exe	764	Services	0	5,044 K	
svchost.exe	848	Services		12,404 K	
svchost.exe	888	Services	0	10,216 K	
dwm.exe	964	Console	1	47,240 K	
svchost.exe	332	Services	0	13,624 K	
svchost.exe	664	Services	0	10, 128 K	
svchost.exe	912	Services	0	5,728 K	
svchost.exe	884	Services	0	7,784 K	

Step 2 View the network analysis result to check whether abnormal IP addresses are connected to the host.

Query command: netstat -ano

- 1. Based on the query result, locate the suspicious addresses that are neither service connection ports nor external addresses used for service connections.
- 2. Check whether the suspicious address is an international address of malicious or abnormal services.
- 3. Locate the target process (for example, **vchost.exe**) from the query result based on the PID value of the abnormal connection (for example, **2240**).

C:\Users	s\Administrator>netstat	-ano		
Active (Connections			
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	848
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	332
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5986	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	INSTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	448
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1100
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1616
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2196
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2580
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	2392
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	592
TCP	0.0.0.0:49696	0.0.0.0:0	LISTENING	600
TCP	192.168.1.125:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.125:49672	100. 125. 11. 131:10180	ESTABLISHED	2240
TCP	[::]:135	[::]:0	LISTENING	848
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:3389	[::]:0	LISTENING	332
TCP	[::]:5357	[::]:0	LISTENING	4
	5 3			

Step 3 Check for abnormal users.

1. Run the following command: **net user**

2. Run the following command to query the time when the user changed the host password: **net user** *username* (for example, **administrator**)

Administrator: Command Prompt	
C:\Users\Administrator>net u User name Full Name Comment	user Administrator Administrator
User's comment Country/region code Account active Account expires	000 (System Default) Yes Never
Password last set Password expires Password changeable Password required User may change password	8/20/2024 10:15:45 AM Never 8/20/2024 10:15:45 AM Yes Yes
Workstations allowed Logon script User profile Home directory	A11
Last logon Logon hours allowed	9/4/2024 2:49:14 PM A11

3. Run the following command to check whether the system has been restarted: **systeminfo**

After a host is restarted, data is automatically deleted. To query file directories, perform **Step 4**.



Step 4 Check for abnormal files.

Run the following command: dir /s file_directory (for example, C:) | findstr "exe"

Query the **.exe** files and directories in a disk (for example, **C**:). Based on the query result, locate abnormal files that are not system files or application-created files. Lock abnormal files.

C:\User=\Administrator>dir /= c: lfin	late "avad
01/06/2022 11:21 AM <dir></dir>	ServerManager, exe StrongName m3xk0k0uc10o.13ai2hibnhnv4xobnimi
Directory of C:\Users\Administrator	AppData\Local\Microsoft_Corporation\ServerManager.exe_StrongName_m3xk0k0ucj0oj3ai2
v4xobnimd	
Directory of C: Users Administrator	AppData\Local\Microsoft_Corporation\ServerManager.exe_StrongName_m3xkOkOucj0oj3ai2
V4x0DD1m3\10.0.0.0	
12/00/2022 OSI2/ PR ADIR/	Indexed DD
Directory of Citogers (Administrator	Applata (Local (Packages (Microsoft, Windows, Cortana_cwonin2txyewy (Applata (Indexed DB
	A Transie drug (transie)
	A (14674872-0187-4887-8744-788148810987) -bernar -see
0823128082 11:18 XB 18:8	A (IACIAE77-0087-4850-5744-285148519857) clearmer ave
08/31/2024 11:15 AM 16.5	14 [1AC14E27-02E7-4E5D-B244-2E51AE519357] cmd exe
08/31/2024 11:15 AM 16.5	(IACI4E77-02E7-4E5D-B744-2E5IAE519357) dfreui exe
08/31/2024 11:15 AM 16.5	54 (1AC14E77-02E7-4E5D-B744-2E51AE5193B7) _1=c=1cp1_exe
08/31/2024 11:15 AM 16.5	54 (1AC14E77-02E7-4E5D-B744-2EB1AE5198B7)magn1fy_exe
08/31/2024 11:15 AM 16.5	54 [1AC14E77-02E7-4E5D-B744-2EB1AE5198B7] [MdSched_exe
08/31/2024 11:15 AM 16.5	54 (1AC14E77-02E7-4E5D-B744-2EB1AE5198B7) _meconfiz_exe
08/31/2024 11:15 AM 16.5	54 (1AC14E77-02E7-4E5D-E744-2EE1AE5198E7)_meinfo32_exe
08/31/2024 11:15 AM 16.5	34 (1AC14877-0287-485D-8744-2881A8519887)_mspaint_exe
08/31/2024 11:15 AM 16.5	34 [AC14877-0287-485D-8744-2881A8519887]_narrator_exe
08/31/2024 11:15 AM 16.5	54 [1AC14877-0287-485D-8744-2881A8519887]_notepad_exe
9873173934 11:15 AB 15:5	34 (1AC14E77-02E7-4E5D-B744-2E5198E7)_odbcad32_exe
98/31/3934 11:15 AB 15:5	34 (1AC14E77-02E7-4E5D-B744-2E5198E7)_osk_exe
20/01/2028* 1112 08 12:2	14 LINCIADI - VEDI - ADDU-DIAA- 200 LADDI 200 // _Der_exe
287.817.828.9 1118 28 118 28	24 (19214011-0301-4055-0144-3001905130011-VecoAetAntrAeTexe
- · · · · · · · · · · · · · · · · · · ·	A LIACIAR 77 - VED / - ADDI / BAR SDE IADDI 100 / J - OUTYETMANAUT - SE
3898193833 1111E XB 1212	A TIACTARY 22-0202-ARED-0244-20014061500021 ad a 22 and a
232251252557 1111E XH 121E	A DIACIAR22_0982_ARED_8244_9881ARE189821 Windows She11 at 0 commonly 11 are
0823123034 11116 XB 16.6	4 (1AC14E72-02E7-4E5D-E744-2EE1AE5198E2) WindowsPowerShell v1 0 PowerShell ISE exe
0873172024 11116 AM 16.6	34 [1AC14E77-02E7-4E5D-B744-2EB1AE5198E7] where they are
0873172024 11116 AM 16.6	4 (6D209377-6AF0-4448-2957-A3773F02200E) Common Files Microsoft Shared Ink min eve
0873172024 11:15 AM 16:5	34 (6D809377-6AF0-4448-8957-A3773F02200E) HestQuard unins000 exe
08/31/2024 11:15 AM 16,5	34 [6D809377-6AF0-4448-8957-A3773F02200E]_Windows NT_Accessories_wordpad_exe
08/31/2024 11:15 AM 16,5	34 [D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27]_odbcad32_exe
08/31/2024 11:15 AM 16,5	34 [D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27] _VindowsPowerShe11_v1_0_powershe11_exe
- 08/31/2024 11-15 AB 16.5	<pre>34 UD5523180-82F1-4857-A4CE-A8E7C5EA7D27)_WindowsPowerShe11_v1_0_PowerShe11_ISE_exe</pre>
1.0 1	

NOTE

You are advised to check the following directories: windows, windows\system32, windows/system32 \drivers, c:\program files\internet explorer/, c:\program files \internet explorer/plugin, and c:\program files\common files\microsoft shared.

- **Step 5** View the Windows host login log (login success event ID: **4624**) to check for abnormal logins to the host.
 - Open Control Panel, choose Administrative Tools > Computer Management > System Tools > Event Viewer > Windows Logs > Security, and click Filter Current Log on the right.
 - 2. Enter **4624** in the **Includes/Excludes Event IDs** box.

Figure 5-11 Filtering current logs

Event Viewer (Local) S	ecuri			Actions
Custom Views	eywo	1	^	Security
Application Security System Provarded Events Applications and Services Lo Subscriptions	Au Filter XML Au Logged: Au Event level: Au & Event level: Au & By log Au & By source Au & By source Au Includes/Exclu Au au Task category: Au Keywords: vent User: Gen Computer(s): A Log Sou	Any time Critical Warning Verbose Error Information Event logs: Security vert sources: des Event IDs: Enter ID numbers and/or ID ranges separated by commas. To a, type a minus sign first. For example 1,3,5-99,-76 d624 cAll Users> cAll Users> cAll Computers> Clear 798 Task Category: User Account Management formation formation Kerwords: Audif Success		 Open Saved Log Create Custom View Import Custom View Clear Log Filter Current Log Properties Find Save All Events As Attach a Task To this L View Refresh Save Selected Events Refresh Help

3. The query results are displayed. See Figure 5-12.

Figure 5-12 Viewing results

- 1	Security Numb	er of events: 32,6	56					Actions	
	Filtered: Log	: Security; Source	: ; Event ID: 4624	Number of events: 104				Security	
	Keywords	Date and Time		Source	Event ID	Task Category	^	👩 Oper	n Saved Log
	Audit Success	9/4/2024 2:49:1	4 PM	Microsoft Win	4624	Logon		Y Crea	te Custom Vier
	Audit Success 9/4/2024 2:48:3		6 PM	Microsoft Win	4624	4624 Logon		Impo	ort Custom Vie
	Audit Success	9/4/2024 2:48:3	5 PM	Microsoft Win	4624	Logon		Clear	rlog
vices I o	Audit Success	9/4/2024 2:48:3	3 PM	Microsoft Win	4624	Logon			Cogin
VICES LO	Audit Success	9/4/2024 2:48:3	3 PM	Microsoft Win	4624	Logon		Pitter	Current Log
	Audit Success	9/4/2024 2:48:3	3 PM	Microsoft Win	4624	Logon		Clear	r Filter
	Audit Success	9/4/2024 2:48:3	3 PM	Microsoft Win	4624	Logon		Prop	erties
	Audit Success	9/4/2024 2:48:3	2:48:33 PM	Microsoft Win	4624	Logon		00 Find.	
	Audit Success	Audit Success 9/4/2024 2:48:33 PM Microsoft Win 4624 Logon							Filtered Log Fi
	Event 4624, Microsoft Windows security auditing.						Atta	ch a Tack To th	
	General Detail	s						TI Save	Filter to Custo
	Friendly View O XMI View						View	,	
	LOG	ongula	10000000	J-0000-0000-0000-0	000000000			G Refre	esh
	TransmittedServices								
	I answitzerselverse							in the p	50.
	Kan	ackagerian	0					Event 462	4, Microsoft W
	Rey	Length	0					Even	t Properties
	Pro	cessid	0x85c					D Atta	ch Task To This
	Pro	cessName	C:\Windov	vs\System32\svchost	.exe			Do Com	
	IpA	ddress	127.0.0.1						·
	IpP	ort	0					be save	Selected Even
	Imp	ersonation	level %%183	3				C Refre	esh
	Res	trictedAdmi	nMode -					Help	
	Tan	aetOuthoun	dilserName	-		~	e0.		
	-	- ·	- · · ·					1	

Step 6 If the problem persists, you can submit a service ticket.

----End

5.2.2.3 Security Hardening Suggestions for Windows Hosts

- Configure security groups and open only necessary ports to the public network. Protect the service web console ports and LAN internal communication ports from being exposed to the public network. Disable highrisk ports (135, 139, and 445) or allow limited source IP addresses to access the ports.
- Do not run applications using the administrator account. Disallow applications (such as webs) to use the database administrator account to interact with databases.

- Periodically back up service data remotely to prevent data loss caused by intrusions.
- Periodically detect security vulnerabilities in the system and software, update system security patches in a timely manner, and upgrade the software to the latest official version.
- Download and install the software from official channels. For the software downloaded from non-official channels, use antivirus software to scan it before running.
- Do not open suspicious email links or web page links.
- Do not use the default password or a weak password for the default account.
- Set OS system passwords (including administrators and common users) and database account passwords. Set strong passwords for the management account of the web application system. The passwords must contain at least 12 characters.
- To improve password strength,
 - Do not use empty passwords or default passwords.
 - Set a long and complex password.
 - Do not set duplicate consecutive characters (for example, AAAAAAAA) or a combination of repeated characters (for example, 123123).
 - Use complex combinations. For example, ensure that your password contains uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and special characters.
 - Do not use the name, date of birth, commemorative date, login name, email address, or words in the dictionary.
 - Do not use common acronyms or abbreviations, for example, **passwd**.
 - Change the password periodically.
 - Do not contain Huawei or adjacent characters on the keyboard, for example, 123qwe!@# and passwd.

5.3 Host Security Check (Linux)

5.3.1 Troubleshooting Methods

You need to check both the users and applications of your Linux hosts.

- **Users**: Check processes and networks and view the users of the running processes. Check for abnormal files in the username directory under the / home directory, and check for abnormal logins and brute-force attacks.
- **Applications**: Check whether abnormal files exist in the directory of the application to which a process belongs.

5.3.2 Troubleshooting Process

This section describes how to troubleshoot security issues in a Linux host.

Procedure

Step 1 Check whether abnormal processes exist in the host.

Query command: top

Check whether abnormal processes exist based on the CPU usage and process names. For example, the CPU usage of the following suspicious process exceeds 100%:

top -	15:26:5	5 up 5	5 day	s, 21:08	3, 3 us	ers, l	oad	d aver	age:	3.54, 3.36	5, 3.29	
Tasks	: 115 to	tal,	1 r	unning,	114 sle	eping,	(ð stop	ped,	0 zombie		
%Cpu(:	s): 100.0	us,	0.0	sy, 0.6	ð ni, 0	.0 id,	0	.0 wa,	0.0	hi, 0.0	si, 0.0	st
KiB M	em : 38	79812	tota	1, 528	8 792 fre	e, 176	96	56 use	d, 1	581364 buf	f/cache	
KiB Sı	wap: 5	24284	tota	1, 208	8680 fre	e, 31	566	04 use	d. 1	124856 ava	il Mem	
PID	USER	PR	NI	VIRT	RES	SHR	s	%CPU	%MEM	TIME+	COMMAND	
25267	oracle	20	0	824248	270772	3480	S 2	149.2	7.0	4540:04	logind	
13493	oracle	20	0	315280	266712	1384	S	50.2	6.9	3728:28	[kthread	di]
2107	oracle	-2	0	1790412	1364	1168	S	0.3	0.0	9:19.83	oracle	
2120	oracle	20	0	1795020	27780	23392	S	0.3	0.7	13:02.99	oracle	

Step 2 Check the file directory based on the PID of the abnormal process.

Query command: **lsof -p** *PID* (for example, 25267)

[root@h		'~]#	lsof	-p25267				
COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
logind	25267	oracle	cwd	DIR	253,1	4096	249 <mark>5</mark> 248	/home/oracle/.config
logind	25267	oracle	rtd	DIR	253,1	4096		
logind	25267	oracle	txt	REG	253,1	7805520	249 <mark>5</mark> 251	/home/oracle/.config/logind
logind	25267	oracle	mem	REG	253,1	109976	183 <mark>6518</mark>	/usr/lib64/libresolv-2.17.so
logind	25267	oracle	mem	REG	253,1	31344	1836506	/usr/lib64/libnss_dns-2.17.so
logind	25267	oracle	mem	REG	253,1	61560	1836508	/usr/lib64/libnss_files-2.17.so
logind	25267	oracle	mem	REG	253,1	2156344	1836490	/usr/lib64/libc-2.17.so
logind	25267	oracle	mem	REG	253,1	1136944	1836498	/usr/lib64/libm-2.17.so
logind	25267	oracle	mem	REG	253,1	19248	1836496	/usr/lib64/libdl-2.17.so
logind	25267	oracle	mem	REG	253,1	43712	1836520	/usr/lib64/librt-2.17.so
logind	25267	oracle	mem	REG	253,1	142144	1836516	/usr/lib64/libpthread-2.17.so
logind	25267	oracle	mem	REG	253,1	163312	1844706	/usr/lib64/ld-2.17.so
logind	25267	oracle	Ør	CHR	1,3	0t0	1031	/dev/null
logind	25267	oracle	lw	CHR	1,3	0t0	1031	/dev/null
logind	25267	oracle	2w	CHR	1,3	0t0	1031	/dev/null
logind	25267	oracle		a_inode	0,10		6394	[eventpoll]

Step 3 Locate abnormal files, which are marked with **xmr** or **mine**.

1. View files: **ll** -art

[root@		1.0	config]#]	ll -art				
total 13670	5							
-rwxrwxrwx	1	oracle	oinstall	54	Jan	9	200:	start
-rwxrwxrwx	1	oracle	oinstall	838583	Jun	15	201	h64
-rwxr-xr-x	1	oracle	oinstall	337	Feb	14	2020	go
-rwxxx	1	oracle	oinstall	215960	Dec	19	2020	arm
-rwxxx	1	oracle	oinstall	5092504	Dec	19	2020	xmrigMiner
-rwxr-xr-x	1	oracle	oinstall	7805520	Apr	28	13:30	logind
-rwxrwxrwx	1	oracle	oinstall	243	Apr	28	13:3:	. update
drwxr-xr-x	2	oracle	oinstall	4096	Jun	25	00:2!	
-rwxrwxrwx	1	oracle	oinstall	392	Jun	25	00:3:	libs
-rw-rr	1	oracle	oinstall	21	Jun	27	11:5 <mark>9</mark>) dir.dir
-rw-rr	1	oracle	oinstall	51	Jun	27	11:5 <mark>9</mark>	cron.d
-rwxrr	1	oracle	oinstall	212	Jun	27	11:5 <mark>9</mark>) upd
-rwxr-xr-x	1	oracle	oinstall	6	Jun	27	11:59	bash.pid
-rw-rr	1	oracle	oinstall	2771	Jun	27	11:59	config.json
drwx	5	oracle	oinstall	4096	Jun	28	16:44	
[root@ł		7.0	config]# p	bwd				
/home/oracl	le,	∕.confi	5					
[root@l	_		config]#					

2. Query the Trojan path: pwd

Detect the file that contains abnormal addresses: **strings** *file_name* (for example, config.json) **|grep xmr**

[root@	7 .config]#	pwd	
/home/oracle	e/.config		
[root@r	.config]#	strings config.json	grep xmr
	"url": "xmr.floo	oder.org:80",	
[root@h	7 .config]#	pwd	
/home/oracle	e/.config		

NOTE

You are advised to check the following directories: **/etc** (configuration files), **/tmp** (temporary files), and **/bin** (executable files).

- In user commands, /lib refers to library files, /etc refers to configuration files, and / sbin refers to executable files.
- In management commands, /lib refers to library files, /etc refers to configuration files, /usr/ refers to read-only files, and shared read-only and /usr/local refer to third-party software.
- 3. Check whether the URL (xmr.flooder.org:80) is a mining pool.
- **Step 4** View the permissions of the host user.

Query command: cat /etc/passwd|grep username (for example, bash)

dr-xr-xr-x. 2 root root 16384 Feb 26 12:38 .
[root@hecs-144007 sbin]# cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
csp:x:1000:1000::/home/csp:/bin/bash
oracle:x:1001:1001::/home/oracle:/bin/bash

The **nologin** user does not have the login permission. You are advised to check the users who have the login permission.

Step 5 Check the abnormal login records from the host login logs.

Query command: **cat** *file_name* (for example, **secure**) **|grep Acc|grep** *username* (for example, oracle)

Find the time that the host is usually logged in to from the success login logs, which may be the time when the Trojan is implanted.



Based on the login time, check the login IP addresses and login frequency (including the number of successful or failed logins). If there are a large number of abnormal IP address logins, brute-force attacks may have taken place.

Jun	25	23:15:00	hecs-144007	sshd[13235]:	Failed password for root from 1 33 port 59376 ssh2	
Jun				sshd[13235]:	Connection closed by 1.15. 3 port 59376 [preauth]	
Jun				sshd[13239]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1	
Jun				sshd[13239]:	Failed password for root from 1. 3 port 59464 ssh2	
Jun				sshd[13239]:	Connection closed by 1.15. 3 port 59464 [preauth]	
Dun				sshd[13243]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13243]:	Failed password for root from 1	
Jun				sshd[13243]:	Connection closed by 1.15 3 port 59552 [preauth]	
Jun				sshd[13246]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1	
Jun				sshd[13246]:	Failed password for root from 1. 33 port 59616 ssh2	
Jun				sshd[13246]:	Connection closed by 1.15 33 port 59616 [preauth]	
Jun				sshd[13250]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1	
Jun				sshd[13250]:	Failed password for root from 1. 03 port 59698 ssh2	
Jun				sshd[13250]:	Connection closed by 1.15 3 port 59698 [preauth]	
Jun				sshd[13254]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1	
Jun				sshd[13254]:	Failed password for root from 1 3 port 59778 ssh2	
Jun				sshd[13254]:	Connection closed by 1.15 3 port 59778 [preauth]	
Jun				sshd[13258]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13258]:	Failed password for root from 1. 3 port 59958 ssh2	
Jun				sshd[13258]:	Connection closed by 1.15 33 port 59958 [preauth]	
Jun				sshd[13262]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13262]:	Failed password for root from 1. 3 port 60218 ssh2	
Jun				sshd[13262]:	Connection closed by 1.15 03 port 60218 [preauth]	
Jun				sshd[13265]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13265]:	Failed password for root from 1 3 port 60342 ssh2	
Jun				sshd[13265]:	Connection closed by 1.15 3 port 60342 [preauth]	
Jun				sshd[13269]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13269]:	Failed password for root from 1 33 port 60414 ssh2	
Jun				sshd[13269]:	Connection closed by 1.1	
Jun				sshd[13273]:	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.	
Jun				sshd[13273]:	Failed password for root from 1 3 port 60496 ssh2	
Jun				sshd[13273]:	Connection closed by 1.15 3 port 60496 [preauth]	
Jun				sshd[13277]:	<pre>pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1.</pre>	
Jun				sshd[13277]:	Failed password for root from 1. 3 port 60606 ssh2	
Jun				sshd[13277]:	Connection closed by 1.1 3 port 60606 [preauth]	

Step 6 If the problem persists, you can submit a service ticket.

----End

5.3.3 Security Hardening Suggestions for Linux Hosts

- Set OS system passwords (including administrators and common users) and database account passwords. Set strong passwords for the management account of the web application system. The passwords must contain at least 12 characters.
- Set the host login mode to key login.
- Do not run applications using the administrator account. Disallow applications (such as webs) to use the database administrator account to interact with databases. Open only necessary ports to the public network. Do not allow public network access to service web console ports and LAN internal communication ports. Disable high-risk ports (such as the SSH port),

allow limited source IP addresses to access the ports, or use the O&M stream established by VPNs or bastion hosts.

- Periodically back up service data remotely to prevent data loss caused by intrusions.
- Periodically detect security vulnerabilities in the system and software, update system security patches in a timely manner, and upgrade the software to the latest official version.
- Download and install the software from official channels. For the software downloaded from non-official channels, use antivirus software to scan it before running.
- You are advised to use HSS to thoroughly detect the potential security risks of your hosts and applications.

For details about HSS, visit https://www.huaweicloud.com/intl/en-us/ product/hss.html.