NOBELIUM targeting delegated administrative privileges to facilitate broader attacks

microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

October 25, 2021

The Microsoft Threat Intelligence Center (MSTIC) has detected nation-state activity associated with the threat actor tracked as NOBELIUM, attempting to gain access to downstream customers of multiple cloud service providers (CSP), managed service providers (MSP), and other IT services organizations (referred to as "service providers" for the rest of this blog) that have been granted administrative or privileged access by other organizations. The targeted activity has been observed against organizations based in the United States and across Europe since May 2021. MSTIC assesses that NOBELIUM has launched a campaign against these organizations to exploit existing technical trust relationships between the provider organizations and the governments, think tanks, and other companies they serve. NOBELIUM is the same actor behind the SolarWinds compromise in 2020, and this latest activity shares the hallmarks of the actor's compromise-one-to-compromise-many approach. Microsoft has notified known victims of these activities through our nation-state notification process and worked with them and other industry partners to expand our investigation, resulting in new insights and disruption of the threat actor throughout stages of this campaign.

Microsoft has observed NOBELIUM targeting privileged accounts of service providers to move laterally in cloud environments, leveraging the trusted relationships to gain access to downstream customers and enable further attacks or access targeted systems. These attacks are not the result of a product security vulnerability but rather a continuation of NOBELIUM's use of a diverse and dynamic toolkit that includes sophisticated malware, password sprays, supply chain attacks, token theft, API abuse, and spear phishing to compromise user accounts and leverage the access of those accounts. These attacks have highlighted the need for administrators to adopt strict account security practices and take additional measures to secure their environments.

In the observed supply chain attacks, downstream customers of service providers and other organizations are also being targeted by NOBELIUM. In these provider/customer relationships, customers delegate administrative rights to the provider that enable the provider to manage the customer's tenants as if they were an administrator within the customer's organization. By stealing credentials and compromising accounts at the service provider level, NOBELIUM can take advantage of several potential vectors, including but not limited to delegated administrative privileges (DAP), and then leverage that access to extend downstream attacks through trusted channels like externally facing VPNs or unique provider-customer solutions that enable network access. To reduce the potential impact of this NOBELIUM activity, Microsoft encourages all of our partners and customers to immediately review the guidance below and implement risk mitigations, harden environments, and investigate suspicious behaviors that match the tactics described in this blog. MSTIC continues to observe, monitor, and notify affected customers and partners through our nation-state notification process. Microsoft Detection and Response Team (DART) and Microsoft Threat Experts have also engaged directly with affected customers to assist with incident response and drive better detection and guidance around this activity.

Post-exploitation patterns against downstream targets

A key trait of NOBELIUM's ongoing activity over the last year has been the abuse of indirect paths and trust relationships to target and gain access to victims of interest for intelligence gain. In the most recent campaign, this has manifested in a compromise-one-to-compromise-many approach—exploiting the service providers' trust chain to gain broad access to multiple customer tenants for subsequent attacks. NOBELIUM leverages established standard business practices, to target downstream customers across multiple managed tenants. These delegated administrative privileges are often neither audited for approved use nor disabled by a service provider or downstream customer once use has ended, leaving them active until removed by the administrators. If NOBELIUM has compromised the accounts tied to delegated administrative privileges through other credential-stealing attacks, that access grants actors like NOBELIUM persistence for ongoing campaigns.

In one example intrusion chain observed by MSTIC during this campaign, the actor was observed chaining together artifacts and access across four distinct providers to reach their end target. The example demonstrates the breadth of techniques that the actor leverages to exploit and abuse trust relationships to accomplish their objective.

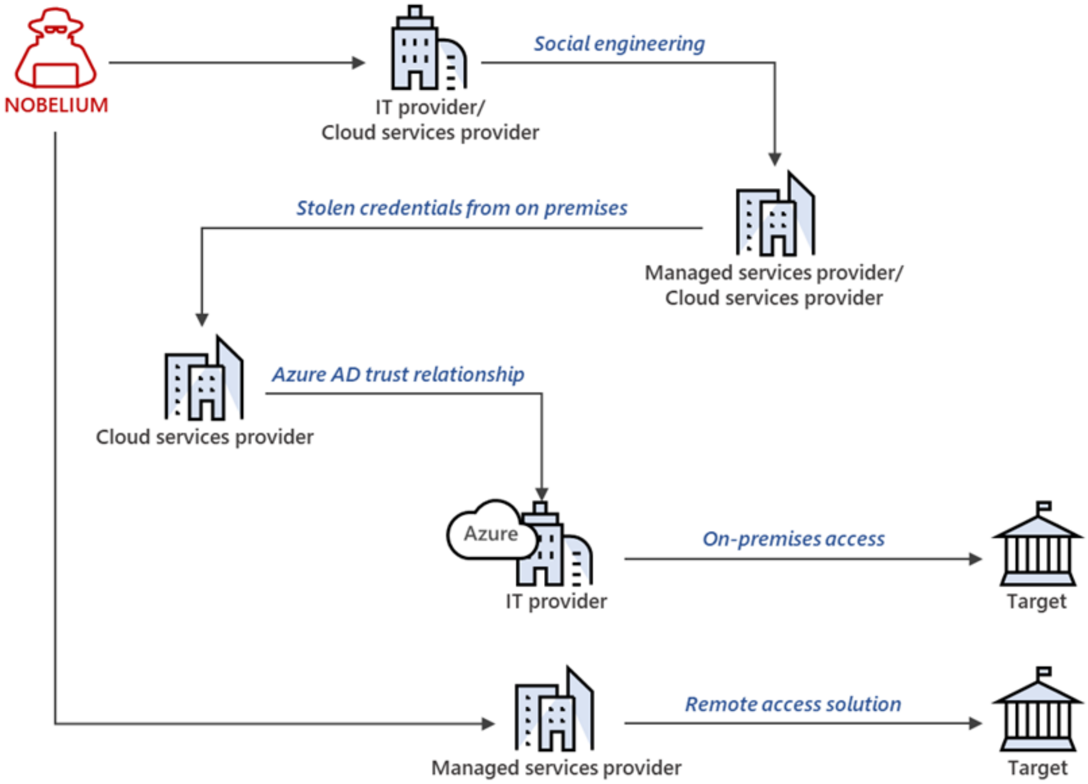


Figure 1: Example intrusion conducted by NOBELIUM demonstrating nested access across variety of methods.

Microsoft assesses that organizations, such as cloud service providers and other technology organizations who manage services on behalf of downstream customers, will be of continued interest to persistent threat actors and are at risk for targeting via a variety of methods, from credential access to targeted social engineering via legitimate business processes and procedures. For additional information on how to identify and triage delegated administrative privileges, see the mitigations and recommendations below.

Mitigation and remediation

Microsoft recommends that cloud service providers, other technology organizations with elevated privileges for customer systems, and all downstream customers of these organizations review and implement the following actions to help mitigate and remediate the recent NOBELIUM activity.

If you are a cloud service provider or an organization who relies on elevated privileges

1. Verify and monitor compliance with Microsoft Partner Center security requirements

All Microsoft partners should review and verify overall compliance status with the partner security requirements through the Microsoft Partner Center. Microsoft recommends the following:

1. **Ensure multifactor authentication (MFA) is in use and conditional access policies are enforced**: All Microsoft partners are required to use MFA to access Partner Center and for cross-tenant access to customer tenants in Microsoft commercial clouds. Partners are advised to check their security compliance in Partner Center and monitor if any user logins or API calls are not compliant with MFA enforcement. Partners should stay compliant at all times.
2. **Adopt the Secure Application Model Framework**: All partners integrating with Partner Center APIs must adopt the Secure Application Model framework for any app and user auth model applications.
3. **Check the Partner Center Activity Logs**: partners are advised to regularly check the "Activity Log" in Partner Center to monitor any user activities, including high privileged user creations, high privileged user role assignment, etc. Partners can also use Partner Center Activity Log APIs to create a custom security dashboard on key user activities in Partner Center to proactively detect suspicious activities.

2. Remove delegated administrative privileges (DAP) connection when not in use

To improve security, Microsoft recommends that partners remove delegated administrative privileges that are no longer in use. Starting in November, a new reporting tool will be available that identifies and displays all active delegated administrative privilege connections and will help organizations to discover unused delegated administrative privileges connections. This tool will provide reporting that captures how partner agents are accessing customer tenants through those privileges and will allow partners to remove the connection when not in use.

1. **We are offering service providers a free two year subscription of Azure Active Directory Premium Plan 2** to further help them manage and get reports on access privileges. Registered partners can log onto Partner Center to take advantage of this offer. Azure AD Premium Plan 2 provides extended access to sign-in logs and premium features such as Azure AD Privileged Identity Management (PIM) and risk-based Conditional Access capabilities to strengthen security controls.

3. Conduct a thorough investigation and comprehensive response.

Carry out additional investigations if you think you might have been affected to determine the full scope of compromised users/assets. Microsoft recommends the following:

1. **Review the Azure AD Security Operations Guide to audit or establish your security operations**. If you are a cloud service provider or an organization that relies on elevated privileges, you need to assess the security implications in your network and its connectivity for your customers. In particular, review authentications that are associated with Azure AD configuration changes using the Microsoft 365 compliance center (formerly in the Exchange admin center) or Azure AD admin logs.
2. **Adequate log retention procedures for cloud-based resources are critical to effectively identify, respond to, and remediate malicious activity**. Cloud service providers and other technology organizations often configure individual subscriptions to meet specific customer requirements. These configurations might not include security controls that enable full accountability to administrative actions should an incident occur. We encourage all organizations to become familiar with logs made available within your subscription and routinely evaluate them for adequacy and anomalies.
3. General Incident response playbooks for Phishing and Password spray are available in Microsoft Security Best Practices.

If you are a downstream customer

1. Review, audit, and minimize access privileges and delegated permissions

It is important to consider and implement a least-privilege approach. Microsoft recommends prioritizing a thorough review and audit of partner relationships to minimize any unnecessary permissions between your organization and upstream providers. Microsoft recommends immediately removing access for any partner relationships that look unfamiliar or have not yet been audited.

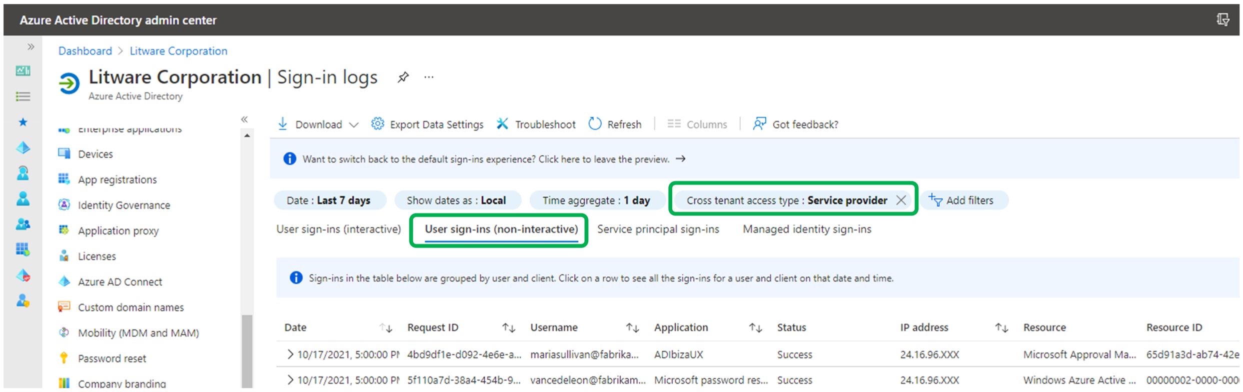
1. **Review, harden, and monitor all tenant administrator accounts**: All organizations should thoroughly review all tenant admin users, including those associated with Administer On Behalf Of (AOBO) in Azure subscriptions and verify the authenticity of the users and activity. We strongly encourage the use of strong authentication for all tenant administrators, review of devices registered for use with MFA, and minimize the use of standing high-privilege access. Continue to reinspect all active tenant admin users accounts and check audit logs on a regular basis to verify that high-privilege user access is not granted or delegated to admin users who do not require these to do their job.
2. **Review service provider permissions access from B2B and local accounts**: In addition to using the delegated administrative privilege capabilities, some cloud service providers use business-to-business (B2B) accounts or local administrator accounts in customer tenants. We recommend that you identify whether your cloud service providers use these, and if so, ensure those accounts are well-governed, and have least-privilege access in your tenant. Microsoft recommends against the use of "shared" administrator accounts. Review the detailed guidance on how to review permissions for B2B accounts.

2. Verify multi-factor authentication (MFA) is enabled and enforce conditional access policies

MFA is the best baseline security hygiene method to protect against threats. Follow the detailed guidance on setting up multifactor authentication in Microsoft 365, as well as the guidance on deploying and configuring conditional access policies in Azure Active Directory (Azure AD).

3. Review and audit logs and configurations

1. **Review and audit Azure AD sign-ins and configuration changes**: Authentications of this nature are audited and available to customers through the Azure AD sign in logs, Azure AD audit logs, and the Microsoft 365 compliance center (formerly in the Exchange Admin Center). We recently added the capability to see sign-ins by partners who have delegated admin permissions. You can see a filtered view of these sign-ins by navigating to the sign-in logs in the Azure AD admin portal, and adding a filter 'Cross-tenant access type: Service provider' on the 'User-sign ins (non-interactive)' tab.



Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 7 days** | Show dates as : **Local** | Time aggregate : **1 day** | Cross tenant access type : **Service provider**

Sign-ins in the table below are grouped by user and client. Click on a row to see all the sign-ins for a user and client on that date and time.

Date	Request ID	Username	Application	Status	IP address	Resource	Resource ID
> 10/17/2021, 5:00:00 PI	4bd9df1e-d092-4e6e-a...	mariasullivan@fabrika...	ADIbizaUX	Success	24.16.96.XXX	Microsoft Approval Ma...	65d91a3d-ab74-42e
> 10/17/2021, 5:00:00 PI	5f110a7d-38a4-454b-9...	vancedeleon@fabrikam...	Microsoft password res...	Success	24.16.96.XXX	Windows Azure Active ...	00000002-0000-000

2. **Review Existing Log Availability and Retention Strategies**: Investigating activities conducted by malicious actors places a large emphasis on having adequate log retention procedures for cloud-based resources including Office 365. Various subscription levels have individualized log availability and retention policies which are important to understand prior to forming an incident response procedure.

We encourage all organizations to become familiar with logs made available within your subscription and routinely evaluate them for adequacy and anomalies. For organizations relying on a third-party organization, work with them to understand their logging strategy for all administrative actions and establish a process should logs need to be made available during an incident.

Observed behaviors and TTPs

Unique indicators (e.g., specific IPs, domains, hashes) have limited value in detecting global NOBELIUM activity because the indicators are mostly compartmented by campaign and specific to the targeted organization. They also regularly obfuscate their attack by shifting infrastructure and maintain very tight operational security around their campaigns. Despite this, the following behaviors and characteristics are common to NOBELIUM intrusions and should be reviewed closely during investigations to help determine if an organization has been affected:

- NOBELIUM leverages “anonymous” infrastructure, which may include low reputation proxy services, cloud hosting services, and TOR, to authenticate to victims
- NOBELIUM has been observed leveraging scripted capabilities, including but not limited to RoadTools or AADInternals, to conduct enumeration of Azure AD, which can result in authentication with user agents of scripting environments
- NOBELIUM has been observed authenticating to accounts from anomalous locations that might trigger impossible travel analytics or fail to pass deployed conditional access policies.
- NOBELIUM has been observed modifying Azure AD to enable long-term persistence and access to sensitive information. This can include the creation of users, consent of Azure AD applications, granting of roles to users and applications, creation of additional service principal credentials, and more. More information at https://aka.ms/nobelium.
- In one incident, MSTIC observed the use of Azure RunCommand, paired with Azure admin-on-behalf-of (AOBO), as a technique to gain access to virtual machines and shift access from cloud to on-premise.
- NOBELIUM has demonstrated an ongoing interest in targeting privileged users, including Global Administrators. Security of at-risk organizations is greatly enhanced by prioritizing events that are detected on privileged accounts.

- NOBELIUM is frequently observed conducting activities consistent with intelligence collection. Routinely monitoring various log sources for anomalies consistent with data exfiltration can serve as an early warning for compromise.
- Organizations previously targeted by NOBELIUM might experience recurring activity and would benefit from implementing proactive monitoring for new attacks.

Detection and Investigation through Advanced Hunting queries

For Microsoft customers using Azure Sentinel, Microsoft 365 Defender, Microsoft Cloud App Security, or registered partners taking advantage of the free two year subscription of Azure Active Directory Premium Plan 2, any of the following in-product detections, investigation guidance, and hunting queries can help organizations accelerate their investigations into this activity.

Azure Sentinel

Azure Sentinel customers can use the following detection queries to look for this activity:

Detections

Name: Azure VM Run Command operations executing a unique PowerShell script
Description: This query identifies when the Azure Run command is used to execute a unique PowerShell script on a virtual machine. The uniqueness of the PowerShell script is determined by taking a combined hash of the cmdlets it imports and the file size of the PowerShell script. Alerts from this detection indicate a unique PowerShell was executed in your environment.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Detections/AzureActivity/RareRunCommandPowerShellScript.yaml

Name: Azure VM Run Command operation executed during suspicious login window
Description: This query identifies when the Azure Run command execution event is associated with a user and IP Address that has recently been associated by an Azure Sentinel UEBA user entity behavior alert.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Detections/MultipleDataSources/RunCommandUEBABreach.yaml

Name: Azure Portal Sign-in from another Azure Tenant
Description: This query looks for sign-in attempts to the Azure Portal where the user who is signing in from another Azure tenant, and the IP address the login attempt is from is an Azure IP. A threat actor who compromises an Azure tenant may look to pivot to other tenants leveraging cross-tenant delegated access in this manner.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Detections/SigninLogs/AzurePortalSigninfromanotherAzureTenant.yaml

Hunting Queries

Name: Azure VM Run Command executed from Azure IP address
Description: This query identifies any Azure VM Run Command operation executed from an Azure IP address. The Run Command allows an attacker or legitimate user to execute arbitrary PowerShell on a target VM.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/AzureActivity/AzureRunCommandFromAzureIP.yaml

Name: Azure VM Run Command linked with MDE
Description: This query identifies any Azure VM Run Command operations and links these operations with MDE host logging. Logging from AzureActivity provides the IP address and user name of the account that invoked the command. The MDE data provides insights into what cmdlets were loaded by the command.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/MultipleDataSources/AzureRunCommandMDELinked.yaml

Name: Dormant Service Principal Update Creds and Logs In
Description: This query look for Service Principal accounts that are no longer used where a user has added or updated credentials for them before logging in with the Service Principal.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/MultipleDataSources/DormantServicePrincipalUpdateCredsandLogsIn.yaml

Name: Dormant User Update MFA and Logs In
Description: This query looks for user accounts that have not been successfully logged into recently, who then have a MFA method added or updated before logging in.
URL: https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/MultipleDataSources/DormantUserUpdateMFAandLogsIn.yaml

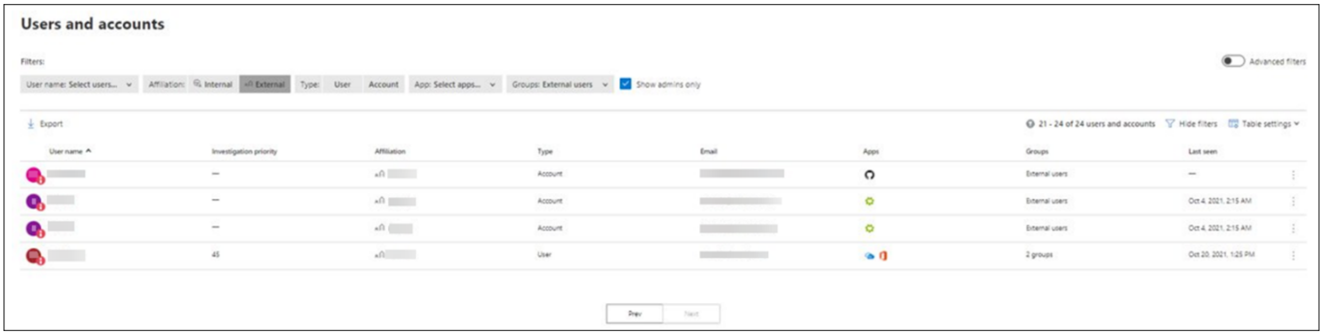
Microsoft 365 Defender

Microsoft 365 Defender provides detection for one of the cloud persistence techniques commonly used by NOBELIUM. That persistence technique relies on maintaining access to victims’ mail system through the modification of permissions and addition of hidden credentials that allow the attacker to access emails remotely. This alert is based on a combination of multiple signals and telemetry that originates from Microsoft Cloud App Security and is triggered either based on the risk score of the account involved or based on the suspicious IP address used to access emails.

Detection Name: Suspicious Addition of an Exchange related App Role
Description: Addition of an Exchange related application role was observed. An account that can authenticate against an application service principal may also be able to access Exchange data and email. This alert was triggered based on another Microsoft Cloud App Security alert related to the potentially compromised user account.

Microsoft Cloud Application Security

Review and audit users and accounts and their activities: Microsoft Cloud App Security provides a quick page to enumerate all the users and accounts but filtering specifically to find "external" users with admin privilege. Once these users and accounts are identified, Cloud App Security can assist to review some of the activities performed and recent sign-ins and risk score.



Users and accounts

Filters:

User name: Select users... | Affiliation: Internal | External | Type: User | Account | App: Select apps... | Groups: External users | ☑ Show admins only

Advanced filters

Export

21 - 24 of 24 users and accounts | Hide filters | Table settings

User name ^	Investigation priority	Affiliation	Type	Email	Apps	Groups	Last seen
[redacted]	—	[redacted]	Account	[redacted]		External users	—
[redacted]	—	[redacted]	Account	[redacted]		External users	Oct 4, 2021, 2:15 AM
[redacted]	—	[redacted]	Account	[redacted]		External users	Oct 4, 2021, 2:15 AM
[redacted]	45	[redacted]	User	[redacted]		2 groups	Oct 20, 2021, 1:25 PM

Prev | Next

Microsoft Cloud App Security also provides detection coverage for some of the NOBELIUM techniques mentioned in earlier sections of this blog, including detection of post-exploitation activities related to manipulation of privileged credentials and a new detection for password-spray typically used to obtain initial foothold.

Detection Name: Activity from password-spray associated IP address
Description: This detection compares IP addresses performing successful activities in your cloud applications to IP addresses identified by Microsoft's threat intelligence sources as recently performing password spray attacks. It alerts about users that were victims of password spray campaigns and managed to access your cloud applications from those malicious IPs.

Detection Name: Unusual addition of credentials to an OAuth app
Description: This detection identifies the suspicious addition of privileged credentials to an OAuth app, based on baseline behavior of activities learned by the product. This can indicate that an attacker has compromised the app, and is using it for malicious activity.

Detection Name: Unusual ISP for an OAuth app
Description: This detection profiles your environment and triggers alerts when OAuth apps perform activities from an unusual ISP, which could indicate an attempted breach using a non-genuine OAuth provider.

Azure Defender

Azure Defender provides detections for abuse of legitimate virtual machine extensions once an attacker has obtained token or valid credentials. Through deep analysis of Azure activity logs, Azure Defender analyzes every call made by authenticated and authorized principals and calculates a likelihood score to determine suspicious intent of the operation and detect it.

Detection Name: Suspicious Run Command invocation detected
Description: Azure Defender for Resource Manager identified a suspicious Run Command invocation in your subscription. Azure Run Command is a feature designed to allow administrators to efficiently manage their environments. While this activity may be legitimate, an attacker with sufficient permissions can utilize Run Command to execute malicious code on your virtual machine. This activity is deemed suspicious as the user rarely invokes operations that enable code execution. This can indicate the account is compromised and is being used with malicious intent.

Microsoft continues to track NOBELIUM's activities, tactics, malware, and tools. We will communicate any additional insights and recommendations as we investigate their actions against our customers. We reinforce the importance of best practice security precautions such as Zero-trust architecture and multi-factor authentication and their importance for everyone. Additional information on best practice security priorities is listed below: