ManageEngine Log360

Products Store Partners Affiliate Support |

Overview Features Demo Resources Get Quote Support Download

Attack detection | Sep 7,2021 | 6 min

Lateral movement: Detecting access token manipulations

Author : Madhuvantii M

Share Tweet Share

Imagine you just landed at your dream tourist destination and want to check in to your pre-booked hotel room. You confirm your identity by showing your passport to the receptionist. The receptionist accepts the proof and gives you the keycard to your room.

Your credentials are similar to a passport; they help confirm, or rather, authenticate, your identity to the server. Windows systems generate access tokens with your security context to give you access to protected resources, very similar to the hotel keycard issued by the receptionist. However, these access tokens can be stolen or manipulated.

Malicious actors want access to your protected resources and will try to impersonate you with stolen access tokens. This article is all about how attackers perform access token manipulation and how you can detect it in your IT environment.

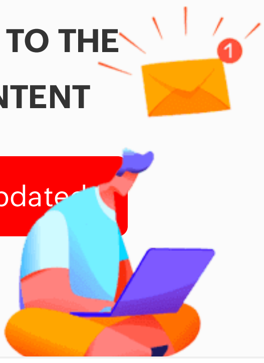
How do access tokens work?

Access tokens are usually issued to Windows processes. They contain a user ID, group ID, privilege, and other security information that cannot be tampered with. When a process tries to access a protected resource, Windows allows the process to do so only if its access token is validated with the access control list of the protected resource. The token that is attached to the initial process is inherited by all child processes. This is a privileged operation that can be carried out from a privileged context, such as an administrator account.

However, Windows has provisions that allow access tokens to be duplicated without any special privilege. For example, to restrict the access of a launched application, new tokens with a lower level of access rights, known as impersonation tokens, are created automatically. Attackers take advantage of these provisions to impersonate a user or system security context, bypass access controls, and perform malicious actions.

What is access token manipulation?

Access token manipulation is when an attacker uses built-in Windows API functions to copy access tokens from existing processes and modify them to suit their purpose. They may apply the stolen tokens to an existing process or use them under a different security context by creating a new process. The following Windows API calls can be used to steal and abuse access tokens: OpenProcess(), OpenProcessToken(), ImpersonateLoggedOnUser(), DuplicateTokenEx(), and CreateProcessWithTokenW().



Related Posts

Evolving cybersecurity threats require SIEM solutions to keep pace

Looking at the digital footprints: Forensic analysis in SIEM

Spotting and stopping cloud attacks: SSH Linux attacks on AWS

other computers in the network in a privileged context. Active Directory fields can also be used to modify access tokens.

Once attackers have these tokens, they access all permitted resources. They may establish access to remote systems or even compromise other systems in your network. Pass-the-hash, pass-the-ticket, and overpass-the-hash are some examples where access token manipulation is used for lateral movement.

Detecting access token manipulation

Access token manipulation techniques are difficult to detect because they leave behind little evidence. Pass-the-ticket attacks are notoriously difficult to detect. However, some actions carried out during access token manipulation generate event logs.

Collecting system event logs and sifting through them for suspicious log patterns can help discover indicators of compromise for some access token manipulation techniques, as tabulated below.

Attack technique	**Indicators of compromise at endpoints**
Pass-the-hash	Check your endpoint logs for: • Windows Event ID 4624 with Logon Type = 9, Authentication package = Negotiate, and Logon Process = seclogo • Sysmon Event ID 10: Process Access to Lsass
Pass-the-ticket	• Check DC logs for: • Windows event IDs in succession: 4768, 4769, 4770

Wrapping up

In short, this is where you can begin to increase your chances of detecting access token manipulation in your environment:

- ✓ Collect logs from all critical systems in your network.
- ✓ Centralize log management for easier access to device logs.
- ✓ Perform event correlation across device logs to detect IoCs.
- ✓ Set up alerts to notify you when suspicious chains of events are found.

While logging can be done with native tools, deploying the right solution can make it much easier and more effective.

ManageEngine Log360 is a comprehensive, easy-to-use SIEM and threat mitigation solution that extensively audits firewalls, routers, switches, applications, file servers, web servers, and much more, giving you complete visibility into your IT environment.

This solution can trigger alerts for IoCs of various attacks and identify malicious traffic connections with its real-time correlation engine. With an Elasticsearch-based search engine, Log360 facilitates drilling down to base logs for further investigation. Log360 also

Get the latest content delivered right to your inbox!

Business Email FR

Keep Me Updated

□ Yes, I would like to receive marketing communication regarding Zoho's products, services, and events from Zoho and its regional partners.

By clicking on **Keep me Updated** you agree to processing of personal data according to the Privacy Policy.

EXPERT TALKS

About us | EULA | Terms of service | Security | Compliance | Privacy policy | Cookie policy |

Affiliate program | Newsletter | Contact sales | Our offices | Global (English)