Detecting Karakurt – an extortion focused threat actor

research.nccgroup.com/2022/02/17/detecting-karakurt-an-extortion-focused-threat-actor/

February 17, 2022

Authored by: **Simon Biggs**, **Richard Footman** and **Michael Mullen**

tl;dr

NCC Group's Cyber Incident Response Team (CIRT) have responded to several extortion cases recently involving the threat actor Karakurt.

During these investigations NCC Group CIRT have identified some key indicators that the threat actor has breached an environment and we are sharing this intelligence to assist the cyber defense security community.

It is thought that there may be a small window to respond to an undetected Karakurt breach prior to data exfiltration taking place and we strongly urge any organisations that use single factor Fortinet VPN access to use the information from the detection section of this blog to identify if they may have been breached.

Initial Access

In all cases investigated, Karakurt have targeted single factor Fortigate Virtual Private Network (VPN) servers.

It was observed that access was made using legitimate Active Directory credentials for the victim environment.

The typical Dwell time (Time from threat actor access to detection) has been in the region of just over a month, in part due to the fact the group do not encrypt their victims and use “living off the land” techniques to remain undetected by not utilising anything recognised as malware.

It is not clear how these credentials have been obtained at this stage with the VPN servers in question not being vulnerable to the high profile Fortigate vulnerabilities that have had attention over the past couple of years.

NCC Group strongly recommends that any organisation utilising single factor authentication on a Fortigate VPN to search for the indicators of compromise detailed at the conclusion of this blog.

Privilege Escalation

Karakurt have obtained access to domain administrator level privileges in all of the investigated cases, but the privilege escalation method has not yet been accurately determined.

In one case, attempts to exploit CVE-2020-1472, also known as Zerologon, were detected by security software. The actual environment was not vulnerable to Zerologon however indicating Karakurt may be attempting to exploit a number of vulnerabilities as part of their operation.

Lateral Movement

Karakurt have then been seen to move laterally onto the primary domain controller of their victim’s using the Sysinternals tool PsExec which provides a multitude of remote functionality.

Karakurt have also utilised Remote Desktop Protocol (RDP) to move around victim environments.

Discovery

Once Karakurt obtain access to the primary domain controller they conduct a number of discovery actions, enumerating information about the domain controller itself as well as the wider domain.

One particular technique involves creating a DNS Zone export via an Encoded PowerShell command.

This command leaves a series of indicators in the Microsoft-Windows-DNS-Server-Service Event Log in the form of Event ID 3150, DNS_EVENT_ZONE_WRITE_COMPLETED.

This log is interesting as an indicator as it was present in all Karakurt engagements investigated by NCC Group CIRT and in all cases the only occurrence of these events were caused when Karakurt performed the zone exports. This was conducted very early in the breach just after initial access and prior to data exfiltration occurring, which was typically two weeks from initial access.

This action is also accompanied by extraction of the NTDS.dit file, believed to be utilised by Karakurt to obtain further credentials as a means of persistence in the environment should the account they initially gained access with be disabled.

This is evident through the presence of logs showing the volume shadow service being utilised.

NCC Group CIRT strongly recommends that any organisation using single factor Fortinet VPN access checks their domain controllers Microsoft-Windows-DNS-Server logs for evidence of Event ID 3150. If this is present at any point since December then it may well be an indicator of a breach by Karakurt.

Data Staging

Once the discovery actions have been completed Karakurt appeared to leave the environment before re-entering and identifying servers with access to sensitive victim data on file shares. Once such a server is identified a secondary persistence mechanism was utilised in the form of the remote desktop software AnyDesk allowing Karakurt access even if the VPN access was removed.

On the same server that AnyDesk is installed Karakurt have been identified browsing folders local to the server and on file shares.

7-Zip archives have then been created on the server.

In the cases investigated there were no firewall logs or other evidence to confirm the data was then exfiltrated but based on the claims from Karakurt along with the file tree text file provided as proof, it is strongly believed that the data was exfiltrated in all cases investigated.

It is suspected that Karakurt are utilising Rclone to exfiltrate data to cloud data hosting providers. This technique was discussed in a previous NCC Group blog, Detecting Rclone – An Effective Tool for Exfiltration

Mitigations

- To remove the threat immediately multi-factor authentication should be implemented for VPN access using a Fortinet VPN.
- Ensure all Domain Controllers are fully patched and patch for critical vulnerabilities generally.

Detection

- Look for evidence of the hosts authenticating from the VPN pool with the naming convention used as default for Windows hosts, for example DESKTOP-XXXXXX.
- Check for event log 3150 in the Microsoft-Windows-DNS-Server-Service Event Log.
- Check for unauthorised use of AnyDesk or PsExec in the environment.