Agenda (Qilin)

By SentinelOne

Published: 2022-11-30 · Archived: 2026-04-05 22:09:03 UTC

Agenda (Qilin) Ransomware: In-Depth Analysis, Detection, and Mitigation

What is Agenda (Qilin) Ransomware?

Agenda ransomware was first observed in July of 2022. Agenda is written in Golang and also referred to as ‘Qilin’. Agenda ransomware supports multiple encryption modes; all of which are controlled by the operator. Agenda actors practice double extortion – demanding payment for a decryptor, as well as for the non-release of stolen data.

What Does Agenda Ransomware Target?

Agenda ransomware is known to target large enterprises and high-value targets. They have also been known to focus on organizations in the healthcare and education sectors in Africa and Asia.

How Does Agenda Ransomware Work?

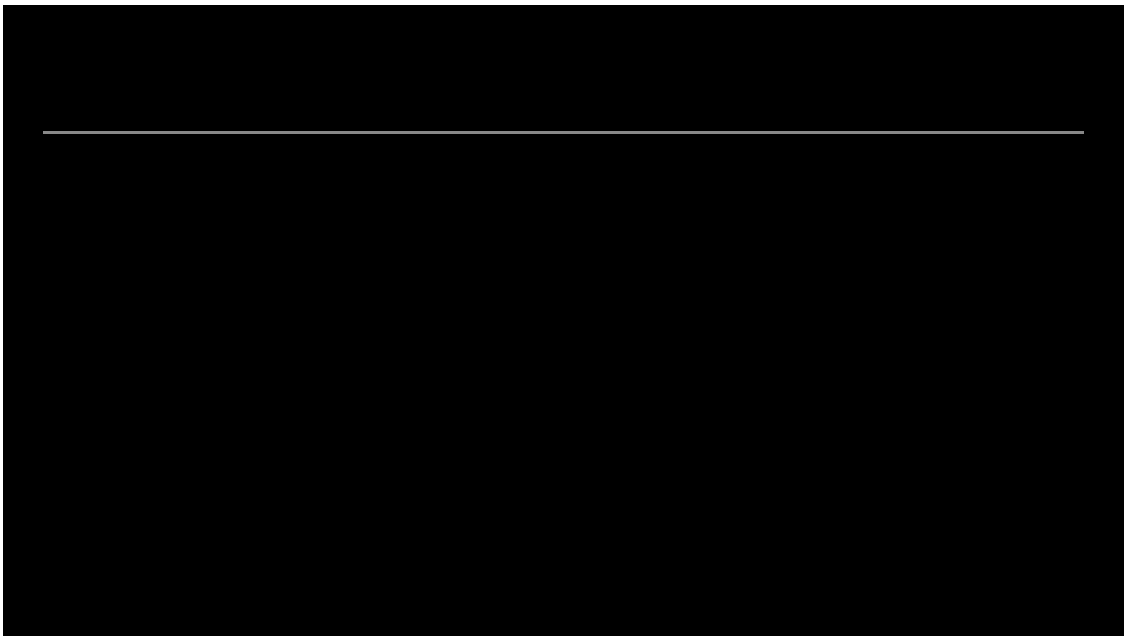
Agenda ransomware targets its victims through phishing and spear phishing emails. They are also known to leverage exposed applications and interfaces such as Citrix and remote desktop protocol (RDP).

Agenda Ransomware Technical Details

Agenda ransomware has some customization options, which include changing the filename extensions of encrypted files and the list of processes and services to terminate. It supports several encryption modes that the ransomware operator can configure through the encryption setting. The ‘help’ screen displays the different encryption modes available: skip-step, percent, and fast.

How to Detect Agenda Ransomware

The SentinelOne Singularity XDR Platform detects and prevents malicious behaviors and artifacts associated with Agenda ransomware.



If you do not have SentinelOne deployed, here are a few ways you can identify Agenda ransomware in your network:

Security Tools

Use anti-malware software or other security tools capable of detecting and blocking known ransomware variants. These tools may use signatures, heuristics, or machine learning algorithms, to identify and block suspicious files or activities.

Network Traffic

Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.

Security Audits

Conduct regular security audits and assessments to identify network and system vulnerabilities and ensure that all security controls are in place and functioning properly.

Education & Training

Educate and train employees on cybersecurity best practices, including identifying and reporting suspicious emails or other threats.

Backup & Recovery Plan

Implement a robust backup and recovery plan to ensure that the organization has a copy of its data and can restore it in case of an attack.

How to Mitigate Agenda Ransomware

SentinelOne Singularity XDR Platform prevents Agenda ransomware infections. In case of an infection, the SentinelOne Singularity XDR Platform detects and prevents malicious behaviors and artifacts associated with Agenda ransomware.

SentinelOne customers are protected from Agenda ransomware without any need to update or take action. In cases where the policy was set to Detect Only and a device became infected, remove the infection by using SentinelOne's unique rollback capability. As the accompanying video shows, the rollback will revert any malicious impact on the device and restore encrypted files to their original state.

In case you do not have SentinelOne deployed, there are several steps that organizations can take to mitigate the risk of Agenda ransomware attacks:

Educate employees

Employees should be educated on the risks of ransomware, and how to identify and avoid phishing emails, malicious attachments, and other threats. They should be encouraged to report suspicious emails or attachments, and to avoid opening them, or clicking on links or buttons in them.

Implement strong passwords

Organizations should implement strong, unique passwords for all user accounts, and should regularly update and rotate these passwords. Passwords should be at least 8 characters long and should include a combination of uppercase and lowercase letters, numbers, and special characters.

Enable multi-factor authentication

Organizations should enable multi-factor authentication (MFA) for all user accounts, to provide an additional layer of security. This can be done through the use of mobile apps, such as Google Authenticator or Microsoft Authenticator, or the use of physical tokens or smart cards.

Update and patch systems

Organizations should regularly update and patch their systems, to fix any known vulnerabilities, and to prevent attackers from exploiting them. This includes updating the operating system, applications, and firmware on all devices, as well as disabling any unnecessary or unused services or protocols.

Implement backup and disaster recovery

Organizations should implement regular backup and disaster recovery (BDR) processes, to ensure that they can recover from ransomware attacks or other disasters. This includes creating regular backups of all data and systems and storing these backups in a secure, offsite location. The backups should be tested regularly to ensure that they are working and that they can be restored quickly and easily.

Qilin (Agenda) Ransomware FAQs

What is Qilin (Agenda) Ransomware?

Qilin, also known as Agenda, is a ransomware family that first appeared in July 2022. It's written in Go (Golang) and later versions in Rust, allowing for cross-platform attacks. Qilin operates as a Ransomware-as-a-Service (RaaS), enabling affiliates to customize attacks based on specific environments. The ransomware employs double extortion tactics, encrypting files and threatening to release stolen data if the ransom isn't paid.

Who is behind the Qilin (Agenda) Ransomware group?

Qilin operates as a Ransomware-as-a-Service (RaaS) affiliate program. The group's origins are linked to Russian-speaking cybercriminal forums, where they recruit affiliates to deploy ransomware attacks. Affiliates receive a percentage of the ransom payments, typically between 80-85%.

How does Qilin (Agenda) Ransomware spread?

Qilin ransomware spreads through phishing and spear-phishing emails containing malicious attachments or links. It also exploits exposed applications and interfaces, such as Citrix and Remote Desktop Protocol (RDP), to gain initial access. Once inside, it leverages tools like Cobalt Strike for deployment and lateral movement within the network.

Which operating systems are targeted by Qilin (Agenda) Ransomware?

Qilin ransomware targets multiple operating systems, including Windows and Linux. It has been observed propagating to VMware vCenter and ESXi servers, affecting virtual environments. The use of Go and Rust programming languages allows for cross-platform compatibility, enhancing its reach.

What types of files does Qilin (Agenda) Ransomware encrypt?

Qilin ransomware encrypts a wide range of file types, focusing on documents, databases, images, and other critical data. It will disrupt operations and pressure victims into paying the ransom to regain access to their essential files.

What encryption algorithms does Qilin (Agenda) Ransomware use?

Qilin ransomware employs multiple encryption algorithms, including ChaCha20, AES-256, and RSA-4096.

Does Qilin (Agenda) Ransomware disable security tools and antivirus software?

Yes, Qilin ransomware attempts to disable security tools and antivirus software to evade detection and facilitate its encryption process. It may terminate specific processes and services, delete system logs, and use obfuscation techniques to avoid identification by security solutions.

What security best practices help prevent Qilin (Agenda) Ransomware infections?

Good security practices to prevent Qilin ransomware infections include conducting regular security audits, monitoring network traffic for unusual activity, and segmenting networks to limit lateral movement. Ensure that Remote Desktop Protocol (RDP) and other remote access points are securely configured and monitored.

Can EDR solutions stop Qilin (Agenda) Ransomware?

Yes. SentinelOne Singularity XDR can stop Qilin (Agenda) ransomware attacks.
