Deloitte. DISP

Actor Details

agrius TLP Amber : **Sophistication Level:** Advanced

Date Updated: 2021-06-29 - 14:12

Last Known Activity: 2021-05

Community Identifiers :

agrius

ActorType: Spy,Nation-State

Description:

Agrius is a suspected state-sponsored Iranian threat group that has been active since at least early 2020 targeting Israeli citizens and companies. The thre at actors initially conducted cyber espionage campaigns, but then they shifted their attacks to extort their targets, claiming to have stolen and encrypted th eir data. This group utilizes VPN services (primarily ProtonVPN) for anonymization when accessing the public facing application of its targets. Agrius' intrusi ons heavily rely on the deployment of webshells, primarily ASPXSpy, ransomware and data wipers. This group is known for having developed the backdoor IPSec Helper and the Apostle wiper and ransomware.

Relevant Information:

- According to reports, the motivation behind Agrius attacks is unlikely to be financial gain due to the fact that the threat actors use both ransomware and wiper malware. This may indicate that the group is hiding its state-sponsored activities using ransomware to make it appear as financially motivated. - The threat group has been observed exploiting publicly available 1-day exploits in web-based apps or using SQL injection for initial access. - Upon successful ex ploitation, Agrius usually uploads a webshell to the compromised system, which are used to tunnel traffic into the network in order to leverage compromise d credentials to move laterally using RDP. - Despite Agrius campaigns have been mostly oriented to Israeli targets, the group has also been reported to tar get a nation-owned critical infrastructure facility in the United Arab Emirates.

Associated Group:
pitty tiger,
Suspected Victims : Israel, United Arab Emirates

Quick Links : Events Tools Sources

Events

CAMPAIGN	DATE	DESCRIPTION	MOTIVATIONS
Iranian threat group 'Agrius' targets Israel with custom 'IPsec Helper' backdoor and 'Apostle' wiper that mimics as ransomware	2021-05-26	On May 25, 2021, security vendor Sentinel Labs reported on a new threat group dubbed 'Agrius' that is attributed to Iranian state-sponsored activity, that does not appear to be purely motivated by financial gain, but rather focused on cyberespionage and business disruption. According to the report, the threat group has been active since early 2020 with initial attacks targeting organizations in the Middle East region and has re-focused operations on Israel since December 2020. While initial activity involved espionage; however, recent operations involved the deployment of wiper malware disguised as ransomware attacks. The threat actors deploy data-wiping malware to destroy the targets' IT infrastructure, and then demand a ransom payment in an attempt to mask their attack as ransomware extortion. The threat actors have shifted to a combination of using their own custom toolsets and easily available offensive security software to deploy a custom wiper-turned-ransomware variant dubbed 'Apostle'. The threat actors were also observed to use a second wiper, called DEADWOOD (a.k.a. Detbosit), which has been observed in previous attacks in the Middle East and attributed to Iran.	Revenge

↑ Back to Top

Tools

NAME	DESCRIPTION
deadwood	DeadWood is a wiper used by the threat group known as Agrius. It is written in C++ using the Boost libraries and it has been active since at least 2019.
aspxspy	ASPXSpy is a publicly available Web shell that has been modified by the APT27 group to gain access over the targeted machines. It has been also used by other threat groups such as Chafer and Volatile Cedar.
ipsec_helper	IPSec Helper is a backdoor developed by the threat actor known as Agrius and written in .NET. This malware provides the basic backdoor functionalities and runs as a service.
apostle	Apostle is a ransomware developed in .NET by the Agrius threat group. It was originally a wiper and has been active since at least November 29, 2020.

↑ Back to Top

Sources

1. https://assets.sentinelone.com/sentinellabs/evol-agrius

↑ Back to Top