APT group: Aggah

Names	Aggah *(Palo Alto)*
Country	[Unknown]
Motivation	Information theft and espionage, Financial gain
First seen	2018
Description	(Palo Alto) In March 2019, Unit 42 began looking into an attack campaign that appeared to be primarily focused on organizations within a Middle Eastern country. Further analysis revealed that this activity is likely part of a much larger campaign impacting not only that region but also the United States, and throughout Europe and Asia. Our analysis of the delivery document revealed it was built to load a malicious macro-enabled document from a remote server via Template Injection. These macros use BlogSpot posts to obtain a script that uses multiple Pastebin pastes to download additional scripts, which ultimately result in the final payload being RevengeRAT configured with a duckdns[.]org domain for C2. During our research, we found several related delivery documents that followed the same process to ultimately install RevengeRAT hosted on Pastebin, which suggests the actors used these TTPs throughout their attack campaign. Initially, we believed this activity to be potentially associated with the Gorgon Group. Our hypothesis was based on the high level TTPs including the use of RevengeRAT. However, Unit 42 has not yet identified direct overlaps with other high-fidelity Gorgon Group indicators. Based on this, we are not able to assign this activity to the Gorgon group with an appropriate level of certainty. In light of that, Unit 42 refers to the activity described in this blog as the Aggah Campaign based on the actor's alias "hagga", which was used to split data sent to the RevengeRAT C2 server and was the name of one of the Pastebin accounts used to host the RevengeRAT payloads.
Observed	Sectors: Automotive, Education, Government, Healthcare, Hospitality, Manufacturing, Media, Retail, Technology. Countries: Austria, Bahrain, Brazil, Canada, China, Egypt, France, Germany, India, Ireland, Israel, Italy, Japan, Norway, Romania, Russia, Saudi Arabia, South Korea, Spain, Sweden, Taiwan, UK, UAE, USA.
Tools used	Agent Tesla, Aggah, NanoCore RAT, njRAT, RevengeRAT, Warzone RAT.
Operations performed	Dec 2018 Operation "Roma225" The Cybaze-Yoroi ZLab researchers investigated a recent espionage malware implant weaponized to target companies in the Italian automotive sector. The malware was spread through well written phishing email trying to impersonate a senior partner of one of the major Brazilian business law firms: "Veirano Advogados". <https://yoroi.company/research/the-enigmatic-roma225-campaign/> Jun 2019 The Evolution of Aggah: From Roma225 to the RG Campaign <https://yoroi.company/research/the-evolution-of-aggah-from-roma225-to-the-rg-campaign/> Sep 2019 During our threat monitoring activities, we discovered an interesting drop chain related to the well-known Aggah campaign <https://yoroi.company/research/apt-or-not-apt-whats-behind-the-aggah-campaign/> Jan 2020 Recently, during our Cyber Defence monitoring operations, we spotted other attack attempts directed to some Italian companies operating in the Retail sector. <https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/> Apr 2020 Upgraded Aggah malspam campaign delivers multiple RATs <https://blog.talosintelligence.com/2020/04/upgraded-aggah-malspam-campaign.html> May 2020 During our Cyber Threat Intelligence monitoring we spotted new malicious activities targeting some Italian companies operating worldwide in the manufacturing sector, some of them also part of the automotive production chain. <https://yoroi.company/research/cyber-criminal-espionage-operation-insists-on-italian-manufacturing/> May 2020 In the past months since the Covid-19 outbreak, we have seen an enormous rise in mal-spam campaigns where hackers abuse the pandemic to try and claim victims. One such campaign that we spotted is a new variant of a unique malware loader named 'Aggah'. <https://www.deepinstinct.com/2020/05/25/aghast-at-aggah-teasing-security-controls-with-advanced-evasion-techniques/> Jul 2021 Aggah Using Compromised Websites to Target Businesses Across Asia, Including Taiwan Manufacturing Industry <https://www.anomali.com/blog/aggah-using-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry> Oct 2021 New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses <https://www.riskiq.com/blog/external-threat-management/aggah-clipboard-hijack-crypto/>

	Jun 2022	Operation “Red Deer” <https://perception-point.io/blog/operation-red-deer/>
Information	<https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/>	

Card date: 21 June 2023

TLP: WHITE

Follow us on

Report incidents

+66 (0)2-123-1227

report-dsc@etda.or.th