TA2101, Maze Team - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:47:31 UTC

APT group: TA2101, Maze Team

Names	TA2101 *(Proofpoint)* Maze Team *(self given)* Twisted Spider *(CrowdStrike)* Gold Village *(SecureWorks)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2019
Description	(Proofpoint) Proofpoint researchers recently detected campaigns from a relatively new actor, tracked internally as TA2101, targeting German companies and organizations to deliver and install backdoor malware. The actor initiated their campaigns impersonating the Bundeszentralamt fur Steuern, the German Federal Ministry of Finance, with lookalike domains, verbiage, and stolen branding in the emails. Proofpoint researchers have also observed this actor distributing Maze ransomware, employing similar social engineering techniques to those it uses for Cobalt Strike, while also targeting organizations in Italy and impersonating the Agenzia Delle Entrate, the Italian Revenue Agency. We have also recently observed the actor targeting organizations in the United States using the IcedID banking Trojan while impersonating the United States Postal Service (USPS).
Observed	Sectors: Construction, Education, Energy, Financial, Government, Healthcare, Hospitality, IT, Manufacturing, Media, Non-profit organizations, Oil and gas, Retail, Shipping and Logistics, Technology, Telecommunications, Transportation and Real estate. Countries: Canada, Costa Rica, France, Germany, Italy, South Korea, Thailand, UK, USA.

Tools used	7-Zip, BokBot, BloodHound, Buran, Cobalt Strike, Egregor, Maze, Mimikatz, nmap, PsExec, SharpHound, WinSCP.	
Operations performed	Nov 2019	Allied Universal Breached by Maze Ransomware, Stolen Data Leaked <https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/>
	Dec 2019	Maze Ransomware Demands $6 Million Ransom From Southwire <https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/>
	Jan 2020	Maze ransomware operators have infected computers from Medical Diagnostic Laboratories (MDLab) and are releasing close to 9.5GB of data stolen from infected machines. <https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/>
	Jan 2020	MAZE Relaunches 'Name and Shame' Website <https://www.infosecurity-magazine.com/news/maze-relaunches-name-and-shame/>
	Feb 2020	Breaking the Ice: A Deep Dive Into the IcedID Banking Trojan’s New Major Version Release <https://securityintelligence.com/posts/breaking-the-ice-a-deep-dive-into-the-icedid-banking-trojans-new-major-version-release/>
	Mar 2020	Chubb Cyber Insurer Allegedly Hit By Maze Ransomware Attack <https://www.bleepingcomputer.com/news/security/chubb-cyber-insurer-allegedly-hit-by-maze-ransomware-attack/>
	Mar 2020	The Maze ransomware group attacked the computer systems of Hammersmith Medicines Research (HMR), publishing personal details of thousands of former patients after the company declined to pay a ransom. <https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus>
	Apr 2020	On April 1st, 2020, Berkine became a victim of cyber-attack by the notorious Maze ransomware group that is known for its unique blackmailing practices. <https://www.hackread.com/maze-ransomware-group-hacks-oil-giant-leaks-data/>
	Apr 2020	Drug testing firm sends data breach alerts after ransomware attack <https://www.bleepingcomputer.com/news/security/drug-testing-firm-

	sends-data-breach-alerts-after-ransomware-attack/>
Apr 2020	IT services giant Cognizant suffers Maze Ransomware cyber attack <https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-ransomware-cyber-attack/>
Apr 2020	The Maze Ransomware gang breached and successfully encrypted the systems of VT San Antonio Aerospace, as well as stole and leaked unencrypted files from the company's compromised devices <https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/>
Apr 2020	Chipmaker MaxLinear reports data breach after Maze Ransomware attack <https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/>
May 2020	According to MAZE, egg producer and supplier Sparboe was cracked into on May 1, 2020. As proof of the attack, the threat group has shared a zip file of data it claims was exfiltrated from Sparboe's systems. <https://www.infosecurity-magazine.com/news/maze-claims-ransomware-attack-on-us/>
May 2020	Package delivery giant Pitney Bowes confirms second ransomware attack in 7 months <https://www.zdnet.com/article/package-delivery-giant-pitney-bowes-confirms-second-ransomware-attack-in-7-months/>
May 2020	Ransomware breach of Banco de Costa Rica <https://www.bleepingcomputer.com/news/security/hackers-say-they-stole-millions-of-credit-cards-from-banco-bcr/> <https://cybleinc.com/2020/05/22/maze-ransomware-operators-release-the-banco-de-costa-rica-data-leak-part-3/>
Jun 2020	Cyber extortionists have stolen sensitive data from a company which supports the US Minuteman III nuclear deterrent. <https://news.sky.com/story/hackers-steal-secrets-from-us-nuclear-missile-contractor-11999442>
Jun 2020	The Maze Ransomware operators are claiming to have successfully attacked business services giant Conduent, where they stole unencrypted files and encrypted devices on their network. <https://www.bleepingcomputer.com/news/security/business-services-giant-conduent-hit-by-maze-ransomware/>

Jun 2020	MAZE maintains that it has encrypted and exfiltrated data from New York company Threadstone Advisors using ransomware. <https://www.infosecurity-magazine.com/news/maze-attacks-victoria-beckhams/>
Jun 2020	LG Electronics allegedly hit by Maze ransomware attack <https://www.bleepingcomputer.com/news/security/lg-electronics-allegedly-hit-by-maze-ransomware-attack/>
Jun 2020	Business giant Xerox allegedly suffers Maze Ransomware attack <https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/>
Jun 2020	Maze Ransomware Operators Allegedly Targeted National Highways Authority of India (NHAI) <https://cybleinc.com/2020/07/02/maze-ransomware-operators-allegedly-targeted-national-highways-authority-of-india-nhai-data-leak/>
Jul 2020	Canon hit by Maze Ransomware attack, 10TB data allegedly stolen <https://www.bleepingcomputer.com/news/security/canon-hit-by-maze-ransomware-attack-10tb-data-allegedly-stolen/>
Aug 2020	The Maze hacker gang claims it has infected computer memory maker SK hynix with ransomware and leaked some of the files it stole. <https://www.theregister.com/2020/08/20/maze_crew_sk_hynix/>
Aug 2020	During the monitoring of deepweb and darkweb leaks, our researchers came across the leak disclosure post in which the Maze ransomware operators allegedly breached Hoa Sen Group and claimed to be in possession of the company’s sensitive data. <https://cybleinc.com/2020/08/17/one-of-the-largest-steel-sheet-companies-in-southeast-asia-got-allegedly-breached-by-maze/>
Sep 2020	Fairfax County schools hit by Maze ransomware, student data leaked <https://www.bleepingcomputer.com/news/security/fairfax-county-schools-hit-by-maze-ransomware-student-data-leaked/>
Oct 2020	Maze ransomware is shutting down its cybercrime operation <https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/>
Oct 2020	Ubisoft, Crytek data posted on ransomware gang's site <https://www.zdnet.com/article/ubisoft-crytek-data-posted-on-ransomware-gangs-site/>

	Oct 2020	Egregor Claims Responsibility for Barnes & Noble Attack, Leaks Data <https://threatpost.com/egregor-responsibility-barnes-noble/160401/>
	Nov 2020	350,000 items of personal data compromised in Capcom hack <https://www.nme.com/news/gaming-news/350000-items-of-personal-data-compromised-in-capcom-hack-2818358>
	Nov 2020	Retail giant Cencosud hit by Egregor Ransomware attack, stores impacted <https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/>
	Dec 2020	Kmart nationwide retailer suffers a ransomware attack <https://www.bleepingcomputer.com/news/security/kmart-nationwide-retailer-suffers-a-ransomware-attack/>
	Dec 2020	Egregor Ransomware attacked HR Giant Randstad <https://securereading.com/egregor-ransomware-attacked-hr-giant-randstad/>
	Feb 2021	French Hospital Hit with Egregor Ransomware <https://www.binarydefense.com/threat_watch/french-hospital-hit-with-egregor-ransomware/>
	Feb 2021	Egregor Ransomware Adopting New Techniques <https://blog.morphisec.com/egregor-ransomware-adopting-new-techniques>
	Feb 2022	The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released last night on the BleepingComputer forums by the alleged malware developer. <https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/>
Counter operations	Mar 2021	Alleged Members of Egregor Ransomware Cartel Arrested <https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html>
	Feb 2024	Zeus, IcedID malware gangs leader pleads guilty, faces 40 years in prison <https://www.bleepingcomputer.com/news/security/zeus-icedid-malware-gangs-leader-pleads-guilty-faces-40-years-in-prison/>
Information	<https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us>	

	<https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html>

Last change to this card: 07 March 2024

Download this actor card in PDF or JSON format
