TA505, Graceful Spider, Gold Evergreen

Archived: 2026-04-06 02:06:40 UTC

APT group: TA505, Graceful Spider, Gold Evergreen

Names	TA505 *(Proofpoint)* Graceful Spider *(CrowdStrike)* Gold Evergreen *(SecureWorks)* Gold Tahoe *(SecureWorks)* TEMP.Warlock *(FireEye)* ATK 103 *(Thales)* SectorJ04 *(ThreatRecon)* Hive0065 *(IBM)* Chimborazo *(Microsoft)* Spandex Tempest *(Microsoft)* G0092 *(MITRE)*
Country	Russia
Motivation	Financial crime, Financial gain
First seen	2006
Description	(Proofpoint) Proofpoint researchers track a wide range of threat actors involved in both financially motivated cybercrime and s largest malicious spam campaigns we have ever observed, distributing instances of the Dridex banking Trojan, Locky ransomv Because TA505 is such a significant part of the email threat landscape, this blog provides a retrospective on the shifting malwa Rockloader that appear to be exclusive to this group as well as more widely distributed malware like Dridex and Pony. Where TA505 is arguably one of the most significant financially motivated threat actors because of the extraordinary volumes of mes underground malware scene. At the time of writing, Locky ransomware remains their malware of choice, even as the group co Much of the malware from TA505 has been observed to be distributed using Avalanche, Cutwail (operated by Narwhal Spider) TA505 also has some infrastructure overlap with Buhtrap, Ratopak Spider and Group-IB found several relationships with Silei The Dridex development appears to have been done by a subgroup named Indrik Spider and, by extension, Doppel Spider. See also: Dungeon Spider and FIN11.
Observed	Sectors: Education, Financial, Healthcare, Hospitality, Retail. Countries: Worldwide.
Tools used	Amadey, AndroMut, Bart, CryptoLocker, CryptoMix, Dridex, Dudear, EmailStealer, FlawedAmmyy, FlawedGrace, FlowerPip Philadelphia, Pony, ReflectiveGnome, RockLoader, RMS, SDBbot, ServHelper, Shifu, Snatch, TeslaGun, TinyMet, Zeus, Livi

Operations performed		
	Oct 2017	On October 10, TA505 introduced their first geo-targeted campaign dropping either Locky or The Trick banking <https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times>
	Jun 2018	We first observed an actor embedding SettingContent-ms inside a PDF on June 18. However, on July 16 we obs with an embedded SettingContent-ms file. <https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-
	Nov 2018	Since November 15, 2018, Proofpoint began observing email campaigns from a specific actor targeting large ret <https://www.proofpoint.com/us/threat-insight/post/ta505-targets-us-retail-industry-personalized-attachments>
	Nov 2018	ServHelper and FlawedGrace – New malware introduced by TA505 <https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
	Dec 2018	In mid-December 2018 a spear-phishing campaign was detected as targeting large US-based retailers along with printer, the initial email lured victims into opening an attached malicious Microsoft Word document.
	Dec 2018	Last month, 360 Threat Intelligence Center captured multiple phishing emails sent by TA505 Group to target fin Backdoor at last. <https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently-en/>

	Apr 2019	LOLBins and a New Backdoor Malware <https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-bac
	Apr 2019	While monitoring their activities, we found that the group is still updating their tactics, techniques, and procedur FlawedAmmyy RAT or RMS RAT as payload. By the end of April, we learned that the group started to go after <https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-o
	May 2019	During the last month our Threat Intelligence surveillance team spotted increasing evidence of an operation inte <https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/>
	May 2019	In the last few days, during monitoring activities, Yoroi CERT noticed a suspicious attack against an Italian orga capabilities and its possible attribution, discovering a potential expansion of the TA505 operation. <https://blog.yoroi.company/research/ta505-is-expanding-its-operations/>
	Jun 2019	In June 2019, TA505 appears to have introduced yet another new downloader malware, AndroMut, which has sc <https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downlo
	Jun 2019	Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi <https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new
	Aug 2019	Given the group's active campaigns since our updates in June and July, we continued following their latest camp or the combination of techniques used for deployment, for each campaign. <https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper
	Sep 2019	In September 2019, Proofpoint researchers observed a prolific threat actor, TA505, sending email campaigns tha FlawedAmmyy, Snatch, and SDBbot (a new RAT) as secondary payloads. <https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-do
	Dec 2019	Throughout January 2020, FireEye has continued to observe multiple targeted phishing campaigns designed to d <https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html>
	2019	TA505 hacking crew spent much of 2019 trying to breach South Korea's financial sector <https://www.cyberscoop.com/ta505-south-korea-bank-phishing/>
	2019	In this newly discovered campaign from TA505, threat actors targeted German companies with trojanized emails techniques could easily be applied to any organization. Once the email attachment was activated, a company's secure credentials and credit card data could be transmitte users files, which suggests this recent activity could also lay the groundwork for an infection vector into the com <https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html>
	Jan 2020	Microsoft says that an ongoing TA505 phishing campaign is using attachments featuring HTML redirectors for <https://www.bleepingcomputer.com/news/security/microsoft-detects-new-ta505-malware-attacks-after-short-br
	Apr 2020	TA505 Continues to Infect Networks With SDBbot RAT <https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/>
	Jun 2020	To evade detection, hackers are requiring targets to complete CAPTCHAs <https://arstechnica.com/information-technology/2020/06/to-evade-detection-hackers-are-requiring-targets-to-c
	Oct 2020	Microsoft is warning that cybercriminals have started to incorporate exploit code for the ZeroLogon vulnerabilit <https://www.bleepingcomputer.com/news/security/ransomware-gang-now-using-critical-windows-flaw-in-attac
	Jun 2021	Signed MSI files, Raccoon and Amadey are used for installing ServHelper RAT <https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html>
	Sep 2021	Explosive New MirrorBlast Campaign Targets Financial Companies <https://blog.morphisec.com/explosive-new-mirrorblast-campaign-targets-financial-companies>
	Sep 2021	Whatta TA: TA505 Ramps Up Activity, Delivers New FlawedGrace Variant <https://www.proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-v
	Oct 2021	TA505 exploits SolarWinds Serv-U vulnerability (CVE-2021-35211) for initial access <https://research.nccgroup.com/2021/11/08/ta505-exploits-solarwinds-serv-u-vulnerability-cve-2021-35211-for-
Counter operations	Mar 2010	Zeus botnet dealt a blow as ISP Troyak knocked out <https://www.itworld.com/article/2762789/zeus-botnet-dealt-a-blow-as-isp-troyak-knocked-out.html>
	Oct 2010	Operation "Trident Breach" FBI announces arrests in $70 million cyber-theft <http://edition.cnn.com/2010/CRIME/10/01/cyber.theft/>

	Mar 2012	John Doe lawsuit against the Zeus operator <http://www.zeuslegalnotice.com/images/Debenham_Decl_Part_1.pdf>
	Jun 2014	Operation “Tovar” Dell SecureWorks Contributes to Efforts Targeting Gameover Zeus and CryptoLocker <https://www.secureworks.com/blog/operation-tovar-dell-secureworks-contributes-to-efforts-targeting-gameove <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-
	Dec 2016	FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicio
	Nov 2022	Suspected Zeus cybercrime ring leader ‘Tank’ arrested by Swiss police <https://www.bleepingcomputer.com/news/security/suspected-zeus-cybercrime-ring-leader-tank-arrested-by-sw
Information	<https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter> <https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group> <https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/> <https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20 <https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malwar <https://threatpost.com/ta505-servhelper-malware/140792/> <https://blog.prevailion.com/2020/01/ta-505-global-ransomware-criminals.html> <https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/> <https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/> <https://blog.fox-it.com/2021/12/02/tracking-a-p2p-network-related-to-ta505/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0092/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=0ac7cc26-cb85-42f7-a2c1-41762b2e2541