APT group: Gamaredon Group

Names	Gamaredon Group *(Palo Alto)* Winterflounder *(iDefense)* Primitive Bear *(CrowdStrike)* BlueAlpha *(Recorded Future)* Blue Otso *(PWC)* Iron Tilden *(SecureWorks)* Armageddon *(SSU)* SectorC08 *(ThreatRecon)* Callisto *(NATO Association of Canada)* Shuckworm *(Symantec)* Actinium *(Microsoft)* Trident Ursa *(Palo Alto)* DEV-0157 *(Microsoft)* UAC-0010 *(CERT-UA)* Aqua Blizzard *(Microsoft)*
Country	Russia
Sponsor	State-sponsored, FSB 16th & 18th Centers
Motivation	Information theft and espionage
First seen	2013
Description	(Lookingglass) The Lookingglass Cyber Threat Intelligence Group (CTIG) has been tracking an ongoing cyber espionage campaign named “Operation Armageddon”. The name was derived from multiple Microsoft Word documents used in the attacks. “Armagedon” (spelled incorrectly) was found in the “Last Saved By” and “Author” fields in multiple Microsoft Word documents. Although continuously developed, the campaign has been intermittently active at a small scale, and uses unsophisticated techniques. The attack timing suggests the campaign initially started due to Ukraine’s decision to accept the Ukraine--European Union Association Agreement (AA). The agreement was designed to improve economic integrations between Ukraine and the European Union. Russian leaders publicly stated that they believed this move by Ukraine directly threatened Russia’s national security. Although initial steps to join the Association occurred in March 2012, the campaign didn’t start until much later (mid-2013), as Ukraine and the EU started to more actively move towards the agreement. Russian actors began preparing for attacks in case Ukraine finalized the AA. The earliest identified modification timestamp of malware used in this campaign is June 26, 2013. A group of files with modification timestamps between August 12 and September 16, 2013 were used in the first wave of spear-phishing attacks, targeting government officials prior to the 10th Yalta Annual Meeting: “Changing Ukraine in a Changing World: Factors of Success.”
Observed	Sectors: Defense, Government, Law enforcement, NGOs and diplomats and journalists. Countries: Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Latvia, Malaysia, Netherlands, Nigeria, Norway, Pakistan, Papua New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK, Ukraine, USA, Vietnam.
Tools used	Aversome infector, DessertDown, DilongTrash, DinoTrain, EvilGnome, FRAUDROP, Gamaredon, ObfuBerry, ObfuMerry, PowerPunch, Pteranodon, QuietSieve, RMS, Resetter, SUBTLE-PAWS, UltraVNC.
Operations performed	Apr 2019 — The discovered attack appears to be designed to lure military personnel: it leverages a legit document of the “State of the Armed Forces of Ukraine” dated back in the 2nd April 2019. <https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-ukrainian-mod-campaign/> May 2019 — The Gamaredon attacks against Ukraine doesn’t seem to have stopped. After a month since our last report we spotted a new suspicious email potentially linked to the Gamaredon group. <https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-a-month-later/> Jul 2019 — EvilGnome: Rare Malware Spying on Linux Desktop Users <https://www.intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/> Oct 2019 — Lure documents observed appear to target Ukrainian entities such as diplomats, government employees, military officials, and more. <https://www.anomali.com/blog/malicious-activity-aligning-with-gamaredon-ttps-targets-ukraine#When:15:00:00Z> Nov 2019 — New wave of attacks <https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/>

Dec 2019	Gamaredon APT Improves Toolset to Target Ukraine Government, Military <https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/>
Mar 2020	Moving into March 2020, countries worldwide are still struggling to manage the spread of the viral disease now known as COVID-19. In cyberspace, threat actors are using the topic of COVID-19 to their advantage with numerous examples of malicious activity using COVID-19 as lure documents in phishing campaigns. <https://info.ai.baesystems.com/rs/308-OXI-896/images/COVID-19-Infographic-Mar2020.pdf>
Early 2020	Since the beginning of 2020 there are reports that APT group has taken advantage of the coronavirus pandemic and used it as a lure to attract victims to open malicious attachments sent with spearphishing emails. <https://www.ria.ee/sites/default/files/content-editors/kuberturve/tale_of_gamaredon_infection.pdf>
Apr 2020	The attacks we found all arrived through targeted emails (MITRE ATT&CK framework ID T1193). One of them even had the subject “Coronavirus (2019-nCoV).” <https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/>
Jan 2021	Russia-Sponsored Group Employs Apparently Legitimate Documents Aligned to Growing Hostilities Between Russia and Ukraine <https://www.anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes>
Jul 2021	Shuckworm Continues Cyber-Espionage Attacks Against Ukraine <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine>
Oct 2021	Since October 2021, ACTINIUM has targeted or compromised accounts at organizations critical to emergency response and ensuring the security of Ukrainian territory, as well as organizations that would be involved in coordinating the distribution of international and humanitarian aid to Ukraine in a crisis. <https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/>
Jan 2022	Russia’s Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine <https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/>
Feb 2022	Gamaredon APT utilised new malware payloads to target Ukraine <https://www.izoologic.com/2022/02/23/gamaredon-apt-utilised-new-malware-payloads-to-target-ukraine/>
Feb 2022	Russia’s Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine <https://unit42.paloaltonetworks.com/trident-ursa/>
Mar 2022	Network Footprints of Gamaredon Group <https://blogs.cisco.com/security/network-footprints-of-gamaredon-group>
Apr 2022	Ukraine spots Russian-linked 'Armageddon' phishing attacks <https://www.bleepingcomputer.com/news/security/ukraine-spots-russian-linked-armageddon-phishing-attacks/>
Apr 2022	Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine>
May 2022	Ukraine CERT-UA warns of new attacks launched by Russia-linked Armageddon APT <https://securityaffairs.co/wordpress/131296/breaking-news/cert-ua-warns-armageddon-apt.html>
Jul 2022	Shuckworm: Russia-Linked Group Maintains Ukraine Focus <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/russia-ukraine-shuckworm>
Sep 2022	Gamaredon APT targets Ukrainian government agencies in new campaign <https://blog.talosintelligence.com/gamaredon-apt-targets-ukrainian-agencies/>
Nov 2022	Gamaredon (Ab)uses Telegram to Target Ukrainian Organizations <https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations>
Nov 2022	Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity <https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html>
Jan 2023	Russia-backed hacker group Gamaredon attacking Ukraine with info-stealing malware <https://therecord.media/russia-backed-hacker-group-gamaredon-attacking-ukraine-with-info-stealing-malware/>

	Jan 2024	Operation “STEADY#URSA” Securonix Threat Research Security Advisory: Analysis and Detection of STEADY#URSA Attack Campaign Targeting Ukraine Military Dropping New Covert SUBTLE-PAWS PowerShell Backdoor <https://www.securonix.com/blog/security-advisory-steadyursa-attack-campaign-targets-ukraine-military/>
Counter operations	Jun 2024	Russian hackers sanctioned by European Council for attacks on EU and Ukraine <https://therecord.media/six-russian-hackers-sanctioned-european-council-eu-ukraine>
	Oct 2024	Ukraine sentences two hackers from Russia-linked Armageddon group <https://therecord.media/ukraine-in-absentia-sentencing-russia-armageddon-gamaredon-hackers>
Information	<https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf> <https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/> <https://www.fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis.html> <https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/> <https://www.recordedfuture.com/bluealpha-iranian-apts/> <https://www.ria.ee/sites/default/files/js/tale_of_gamaredon_infection.pdf> <https://blog.talosintelligence.com/2021/02/gamaredonactivities.html> <https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military> <https://www.bleepingcomputer.com/news/security/gamaredon-hackers-start-stealing-data-30-minutes-after-a-breach/> <https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/Gamaredon_activity.pdf> <https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0047/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=tridentursa>	

Card date: 24 October 2024

TLP: WHITE

Follow us on

Report incidents

+66 (0)2-123-1227

helpdesk@etda.or.th