Carbanak, Anunak - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:43 UTC

APT group: Carbanak, Anunak

Names	Carbanak *(Kaspersky)* Anunak *(Group-IB)* Carbon Spider *(CrowdStrike)* Gold Waterfall *(SecureWorks)* ELBRUS *(Microsoft)* Sangria Tempest *(Microsoft)* G0008 *(MITRE)*
Country	Ukraine
Motivation	Financial crime, Financial gain
First seen	2013
Description	Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. (Kaspersky) From late 2013 onwards, several banks and financial institutions have been attacked by an unknown group of cybercriminals. In all these attacks, a similar modus operandi was used. According to victims and the law enforcement agencies (LEAs) involved in the investigation, this could result in cumulative losses of up to 1 billion USD. The attacks are still active. This report provides a technical analysis of these attacks. The motivation for the attackers, who are making use of techniques commonly seen in Advanced Persistent Threats (APTs), appears to be financial gain as opposed to espionage. An analysis of the campaign has revealed that the initial infections were achieved using spear phishing emails that appeared to be legitimate banking communications, with Microsoft Word 97 – 2003 (.doc) and Control Panel Applet (.CPL) files attached. We believe that the attackers also redirected to exploit kits website traffic that related to financial activity.
Observed	Sectors: Energy, Financial, Food and Agriculture, Healthcare, Hospitality. Countries: Australia, Austria, Brazil, Bulgaria, Canada, China, Czech, France,

	Germany, Hong Kong, Iceland, India, Luxembourg, Morocco, Nepal, Norway, Pakistan, Poland, Russia, Spain, Sweden, Switzerland, Taiwan, UK, Ukraine, USA, Uzbekistan.	
Tools used	Antak, Ave Maria, BABYMETAL, Backdoor Batel, Bateleur, BELLHOP, BlackMatter, Boostwrite, Cain & Abel, Carbanak, Cobalt Strike, Clop, DarkSide, DNSMessenger, DNSRat, DRIFTPIN, FlawedAmmyy, FOXGRABBER, Griffon, HALFBAKED, JS Flash, KLRD, Mimikatz, MBR Eraser, Odinaff, POWERPIPE, POWERSOURCE, PsExec, SocksBot, SoftPerfect Network Scanner, SQLRAT, TeamViewer, TinyMet, WARPRISM.	
Operations performed	Aug 2020	DarkSide: New targeted ransomware demands million dollar ransoms <https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/>
	Aug 2020	DarkSide Ransomware hits North American real estate developer <https://www.bleepingcomputer.com/news/security/darkside-ransomware-hits-north-american-real-estate-developer/>
	Oct 2020	Ransomware gang donates part of ransom demands to charity organizations <https://www.zdnet.com/article/ransomware-gang-donates-part-of-ransom-demands-to-charity-organizations/>
	Nov 2020	Darkside Ransomware Gang Launches Affiliate Program <https://www.bankinfosecurity.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968>
	Nov 2020	DarkSide Ransomware Group Makes New Storage System <https://www.binarydefense.com/threat_watch/darkside-ransomware-group-makes-new-storage-system/>
	Feb 2021	Leading Canadian rental car company hit by DarkSide ransomware <https://www.bleepingcomputer.com/news/security/leading-canadian-rental-car-company-hit-by-darkside-ransomware/>
	Feb 2021	Eletrobras, Copel energy companies hit by ransomware attacks <https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/>
	Feb 2021	Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact <https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/>

Mar 2021	Darkside 2.0 Ransomware Promises Fastest Ever Encryption Speeds <https://www.infosecurity-magazine.com/news/darkside-20-ransomware-fastest/>
Mar 2021	CompuCom MSP hit by DarkSide ransomware cyberattack <https://www.bleepingcomputer.com/news/security/compucom-msp-hit-by-darkside-ransomware-cyberattack/>
Apr 2021	Canadian retailer Home Hardware hit by ransomware <https://financialpost.com/technology/tech-news/canadian-retailer-home-hardware-hit-by-ransomware>
Apr 2021	Ransomware gang wants to short the stock price of their victims <https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/>
Apr 2021	US chemical distributor shares info on DarkSide ransomware data theft <https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/>
Apr 2021	Fashion retailer Guess discloses data breach after ransomware attack <https://www.bleepingcomputer.com/news/security/fashion-retailer-guess-discloses-data-breach-after-ransomware-attack/>
May 2021	A Toshiba business unit says it has been attacked by hacking group DarkSide <https://www.cnbc.com/2021/05/14/toshiba-business-unit-says-it-has-been-hacked-by-darkside-reuters.html>
May 2021	Chemical distributor pays $4.4 million to DarkSide ransomware <https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/>
May 2021	Largest U.S. pipeline shuts down operations after ransomware attack <https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/>
Jul 2021	BlackMatter ransomware targets companies with revenue of $100 million and more <https://therecord.media/blackmatter-ransomware-targets-companies-with-revenues-of-100-million-and-more/>
Aug 2021	Linux version of BlackMatter ransomware targets VMware ESXi servers

		<https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/>
	Aug 2021	FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware <https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/>
	Sep 2021	BlackMatter ransomware hits medical technology giant Olympus <https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-hits-medical-technology-giant-olympus/>
	Sep 2021	US farmer cooperative hit by $5.9M BlackMatter ransomware attack <https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/>
	Sep 2021	Marketron marketing services hit by Blackmatter ransomware <https://www.bleepingcomputer.com/news/security/marketron-marketing-services-hit-by-blackmatter-ransomware/>
	Oct 2021	DarkSide ransomware gang moves some of its Bitcoin after REvil got hit by law enforcement <https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/>
	Nov 2021	BlackMatter: New Data Exfiltration Tool Used in Attacks <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration>
	Nov 2021	BlackMatter ransomware moves victims to LockBit after shutdown <https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/>
	Apr 2023	Microsoft: Notorious FIN7 hackers return in Clop ransomware attacks <https://www.bleepingcomputer.com/news/security/microsoft-notorious-fin7-hackers-return-in-clop-ransomware-attacks/>
Counter operations	Mar 2018	Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>
	Aug 2018	Three Carbanak cyber heist gang members arrested <https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested>

	May 2021	Darkside ransomware gang says it lost control of its servers & money a day after Biden threat <https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/>
	Jul 2021	Dutch police confiscate DarkSide server <https://cyberthreatintelligence.com/news/dutch-police-confiscate-darkside-server/>
	Nov 2021	BlackMatter ransomware says its shutting down due to pressure from local authorities <https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/>
	Nov 2021	US offers $10 million reward for info on Darkside ransomware group <https://therecord.media/us-offers-10-million-reward-for-info-on-darkside-ransomware-group/>
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf> <https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf> <https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf> <https://www.databreaches.net/a-chat-with-darkside/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0008/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
