Sprite Spider, Gold Dupont - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:10:19 UTC

APT group: Sprite Spider, Gold Dupont

Names	Sprite Spider *(CrowdStrike)* Gold Dupont *(SecureWorks)*	
Country	[Unknown]	
Motivation	Financial crime, Financial gain	
First seen	2015	
Description	(CrowdStrike) In 2020, CrowdStrike Intelligence observed both SPRITE SPIDER (the operators of Defray777) and Anunak (the operators of DarkSide) deploy Linux versions of their respective ransomware families on ESXi hosts du operations. While ransomware for Linux has existed for many years, BGH actors have historically not targeted Linux ESXi specifically. ESXi is a type of hypervisor that runs on dedicated hardware and manages multiple virtual machir With more organizations migrating to virtualization solutions to consolidate legacy IT systems, this is a natural targe ransomware operators looking to increase the impact against a victim. All identified incidents were enabled by the acquisition of valid credentials. In four separate Defray777 incidents, SP SPIDER used administrator credentials to log in through the vCenter web interface. In one instance, SPRITE SPIDE the PyXie remote access trojan (RAT) LaZagne module to harvest vCenter administrator credentials stored in a web By targeting these hosts, ransomware operators are able to quickly encrypt multiple systems with relatively few actu ransomware deployments. Encrypting one ESXi server inflicts the same amount of damage as individually deploying on each VM hosted on a given server. Consequently, targeting ESXi hosts can also improve the speed of BGH operat Additionally, due to their lack of conventional operating systems, ESXi hosts lack endpoint protection software that or detect ransomware attacks.	
Observed	Sectors: Education, Healthcare, Manufacturing, Technology.	
Tools used	Cobalt Strike, Defray777, LaZagne, Metasploit, PyXie, SharpHound, Shifu, SystemBC, Vatet.	
Operations performed	Aug 2017	New Defray Ransomware Targets Education and Healthcare Verticals <https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-an verticals>
	May 2020	Texas Courts hit by ransomware, network disabled to limit spread <https://www.bleepingcomputer.com/news/security/texas-courts-hit-by-ransomware-network-disal spread/>
	Jun 2020	New Ransom X Ransomware used in Texas TxDOT cyberattack <https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txd cyberattack/>
	Aug 2020	Business technology giant Konica Minolta hit by new ransomware <https://www.bleepingcomputer.com/news/security/business-technology-giant-konica-minolta-hit- ransomware/>
	Sep 2020	SoftServe hit by ransomware, Windows customization tool exploited <https://www.bleepingcomputer.com/news/security/softserve-hit-by-ransomware-windows-custon exploited/>

	Sep 2020	Leading U.S. laser developer IPG Photonics hit with ransomware <https://www.bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-v ransomware/>
	Sep 2020	Government software provider Tyler Technologies hit by ransomware <https://www.bleepingcomputer.com/news/security/government-software-provider-tyler-technolog ransomware/>
	Oct 2020	Montreal's STM public transport system hit by ransomware attack <https://www.bleepingcomputer.com/news/security/montreals-stm-public-transport-system-hit-by- attack/>
	Nov 2020	Brazil's court system under massive RansomExx ransomware attack <https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomex ransomware-attack/>
	Nov 2020	RansomExx ransomware also encrypts Linux systems <https://www.bleepingcomputer.com/news/security/ransomexx-ransomware-also-encrypts-linux-s
	Dec 2020	Hackers leak data from Embraer, world's third-largest airplane maker <https://www.zdnet.com/article/hackers-leak-data-from-embraer-worlds-third-largest-airplane-mal
	Feb 2021	French MNH health insurance company hit by RansomExx ransomware <https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by ransomware/>
	Feb 2021	Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ran Maximize Impact <https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomw
	Jul 2021	Ecuador's state-run CNT telco hit by RansomEXX ransomware <https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx ransomware/>
	Aug 2021	RansomEXX ransomware leaks files stolen from Italian luxury brand Zegna <https://securityaffairs.co/wordpress/120898/data-breach/ransomexx-ransomware-zegna.html>
	Aug 2021	Computer hardware giant GIGABYTE hit by RansomEXX ransomware <https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ran ransomware/>
	Aug 2021	Ransomware hits Lojas Renner, Brazil’s largest clothing store chain <https://therecord.media/ransomware-hits-lojas-renner-brazils-largest-clothing-store-chain/>
	Mar 2022	Ransomware group attacks Scottish mental health charity <https://therecord.media/ransomware-group-attacks-scottish-mental-health-charity/>
	Oct 2022	RansomExx Leaks 52GB of Barcelona Health Centers' Data <https://www.bankinfosecurity.com/ransomexx-leaks-52-gb-barcelona-health-centers-data-a-2026
	Nov 2022	RansomExx Upgrades to Rust <https://securityintelligence.com/posts/ransomexx-upgrades-rust/>
Information	<https://www.neosecuretendencias2021.com/assets/pdfs/crowdstrike/2021%20Global%20Threat%20Report%20FIN <https://www.secureworks.com/research/threat-profiles/gold-dupont>	

Last change to this card: 27 December 2022

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=20947960-7770-472c-8152-4f88a1f7ea69