Nombre de actor

RansomHub

Tipo de amenaza

RaaS

Motivación

Finantian gain

Alias

Línea temporal

Since its inception in February 2024

In October 2024, ReliaQuest responded to an intrusion affecting a manufacturing sector customer. We identified “Scattered Spider” to be behind the incident. This English-speaking collective previously served as an affiliate for ransomware group “ALPHV” and now partners with “RansomHub.”

Países víctima

UK

Nombre víctimas

Christie’s auction house

Sectores afectados

water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors.

Grupos asociados

Scattered Spider, CosmicBeetle, NoName

Contexto de la amenaza

RansomHub is a relatively new but now prolific threat, emerging in February 2024. Its growth in popularity with established ransomware actors coincided with the law enforcement operation against the LockBit RaaS earlier this year. Notably, it forbids affiliates from targeting entities in China, Cuba, North Korea, Romania and Commonwealth of Independent States (CIS) countries.

Despite shared origins, it is unlikely that Knight’s creators are now operating RansomHub. Source code for Knight (originally known as Cyclops) was offered for sale on underground forums in February 2024 after Knight’s developers decided to shut down their operation. It is possible that other actors bought the Knight source code and updated it before launching RansomHub.

The affiliates leverage a double-extortion model by encrypting systems and exfiltrating data to extort victims. It should be noted that data exfiltration methods are dependent on the affiliate conducting the network compromise. The ransom note dropped during encryption does not generally include an initial ransom demand or payment instructions.

typically compromise internet facing systems and user endpoints by using methods such as phishing emails [T1566], exploitation of known vulnerabilities [T1190], and password spraying [T1110.003]

the attackers gained initial access by exploiting the Zerologon vulnerability (CVE-2020-1472)

Información cuantitativa

at least 210 victims

Tecnologías atacadas

Citrix ADC (NetScaler)

FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN

Java OpenWire protocol marshaller, such as in Apache ActiveMQ

Confluence Data Center and Server instances

BIG-IP system

Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and FortiClientEMS 7.0.1 through 7.0.10

SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016

ESXi environment

Bibliografía

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

<https://www.fortinet.com/blog/threat-research/ransomware-roundup-knight>

<https://redskyalliance.org/xindustry/knight-ransomware>

<https://www.uptycs.com/blog/threat-research-report-team/cyclops-ransomware-stealer-combo>

<https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/>

<https://www.security.com/threat-intelligence/ransomhub-knight-ransomware>

<https://www.scworld.com/news/ransomhub-threatens-to-leak-data-of-christies-auction-house-clients>

<https://www.reliaquest.com/blog/scattered-spider-x-ransomhub-a-new-partnership/>

<https://intel471.com/blog/hunting-for-ransomhub-and-antivirus-killers>

<https://www.forescout.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/>

<https://thehackernews.com/2024/09/cosmicbeetle-deploys-custom-scransom.html>

<https://www.bleepingcomputer.com/news/security/noname-ransomware-gang-deploying-ransomhub-malware-in-recent-attacks/>