LoanDepot Compromised by ALPHV/BlackCat Ransomware

Date of Event: January 3-5, 2024

Overview

Between January 3-5, prolific Russian ransomware group ALPHV/BlackCat compromised LoanDepot, a California-based mortgage company, resulting in the exposure of sensitive data associated with approximately 17 million customers, including social security numbers, names, phone numbers, dates of birth, and financial account numbers.[1] On January 4th, LoanDepot filed a SEC Form 8-K, a report filed to notify investors of major events, stating:[2]

> *LoanDepot, Inc. (the "Company") recently identified a cybersecurity incident affecting certain of the Company's systems. Upon detecting unauthorized activity, the Company promptly took steps to contain and respond to the incident, including launching an investigation with assistance from leading cybersecurity experts, and began the process of notifying applicable regulators and law enforcement. Though our investigation is ongoing, at this time, the Company has determined that the unauthorized third party activity included access to certain Company systems and the* ***encryption of data****. In response, the Company shut down certain systems and continues to implement measures to secure its business operations, bring systems back online and respond to the incident. The Company will continue to assess the impact of the incident and whether the incident may have a material impact on the Company.*

ALPHV/BlackCat claimed their negotiations with LoanDepot included a proposed six million dollar ransom. Although unconfirmed, the group alleged that "LoanDepot employed 'stalling tactics' during negotiations and ultimately stopped responding to the group."[3] To date, the compromised LoanDepot data has not been publicly disclosed by ALPHV/BlackCat. The U.S. Department of State has issued a reward in the amount of up to $15 million for information leading to the identification or location of ALPHV/BlackCat leadership.[4]

Outcomes

Adversarial groups, such as ALPHV/BlackCat, frequently target industries known for retaining vast quantities of sensitive personal information, including healthcare, financial, education, and local governments. Sensitive stolen information can be used to facilitate additional criminal activity, such as identity theft and highly targeted social engineering-enabled phishing attacks.[5]

On February 28, 2024, it was announced that President Biden "will issue an executive order Wednesday seeking to restrict the sale of sensitive American data to China, Russia and four more countries [Iran, North Korea, Cuba,

Venezuela], a first-of-its-kind attempt to keep personally identifying information from being obtained for blackmail, scams or other harm."[6] The restrictions will also include entities linked to the aforementioned countries. Restricting the sale of personal data to adversarial countries will likely result in a demand increase for data procured through criminal activity, such as ransomware and data exfiltration.

ALPHV/BlackCat Profile

ALPHV/BlackCat is a Russian ransomware-as-a-service (RaaS) group, established in approximately 2021, that gained international notoriety by using and providing affiliates with the infrastructure that allows operators to launch financially motivated attacks. According to the U.S. Department of Justice, ALPHV/BlackCat is responsible for financial losses in the hundreds of millions. In December 2023, ALPHV/BlackCat's infrastructure was seized as the result of law enforcement action. According to CPO Magazine, "the FBI used a confidential human source to infiltrate the gang after offering rewards of up to $10 million for crucial information related to hacking groups targeting US critical infrastructure."[7] The FBI used the access to retrieve "946 keys used for hosting various communication channels, data leak sites, and affiliate panels. Subsequently, the federal law enforcement agency provided a free decryption tool to over 400 organizations victimized by the BlackCat cyber gang, including schools, healthcare, emergency services, and critical manufacturers."[8]

Following the seizure by law enforcement, ALPHV/BlackCat "has since 'unseized' their sites and switched a new Tor leak site that the FBI has not yet taken down."[9] Additionally, likely in an effort to retain affiliates, ALPHV/BlackCat announced it would allow those affiliates to retain 90% of the ransoms paid as well as authoring a "rant" in Russian stating that previously "off-limits" targets, including hospitals and nuclear power facilities, may now be attacked.[10] Despite the statement, hospitals are a frequent target of ransomware attacks and previous limitations on the sector do not appear to have been enforced.

Tactics, Techniques, & Procedures (TTPs)

On February 27, 2024, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Human and Health Services (HHS) released an update to a joint advisory regarding ALPHV/BlackCat providing new indicators of compromise (IOCs) and TTPs associated with the group.[11] The following was directly lifted from the advisory. See here for full CISA advisory.

- ALPHVBlackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access. Actors pose as company IT and/or helpdesk staff and use phone calls or SMS messages [T1598] to obtain credentials from employees to access the target network [T1586]. ALPHV Blackcat affiliates use uniform resource locators (URLs) to live-chat with victims to convey demands and initiate processes to restore the victims' encrypted files.
- After gaining access to a victim network, ALPHV Blackcat affiliates deploy remote access software such as AnyDesk, Mega sync, and Splashtop in preparation of data exfiltration. ALPHV Blackcat affiliates create a user account, "aadmin," and use Kerberos token generation for domain access [T1558]. After gaining access to networks, they use legitimate remote access and tunneling tools, such as Plink and Ngrok [S0508]. ALPHV Blackcat affiliates claim to use Brute Ratel C4 [S1063] and Cobalt Strike [S1054] as beacons to command and control servers. ALPHV Blackcat affiliates use the open source adversary-in-the-middle attack [T1557] framework Evilginx2, which allows them to obtain multifactor authentication (MFA) credentials, login credentials, and session cookies. The actors also obtain passwords from the domain controller, local network, and deleted backup servers to move laterally throughout the network [T1555].
- To evade detection, affiliates employ allowlisted applications such as Metasploit. Once installed on the domain controller, the logs are cleared on the exchange server. Then Mega.nz or Dropbox are used to move, exfiltrate, and/or download victim data. The ransomware is then deployed, and the ransom note is embedded as a file.txt. According to public reporting, affiliates have additionally used POORTRY and STONESTOP to terminate security processes.

- Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR [S0183], Tox, email, or encrypted applications. The threat actors then delete victim data from the victim's system.
- ALPHV Blackcat affiliates offer to provide unsolicited cyber remediation advice as an incentive for payment, offering to provide victims with "vulnerability reports" and "security recommendations" detailing how they penetrated the system and how to prevent future re-victimization upon receipt of ransom payment. The ALPHV Blackcat encryptor results in a file with the following naming convention: RECOVER-(seven-digit extension) FILES.txt.

Noteworthy Attacks & Victims

ALPHV/BlackCat ransomware has targeted an extensive list of victims representing various sectors, including manufacturing, healthcare, and transportation. According to a Reuters report, ALPHV/BlackCat was recently implicated in a ransomware attack targeting UnitedHealth Group subsidiary, Optum, resulting in outages of payment platforms at pharmacies across the U.S. Previous reports suggested the cyberattack originated from "suspected nation-state."[12] ALPHV/BlackCat did not respond to request from Reuters, when asked if they were responsible for the attacks.[13] The following is a non-exhaustive list of ALPHV/BlackCat ransomware victims.

- **Prudential Financial**: On February 5th, 2024, Prudential Financial filed a SEC Form 8-K disclosing a cyber attack resulting in unauthorized access to certain systems.[14] ALPHV/BlackCat claimed responsibility for the attack.[15]
- **Trans-Northern Pipelines:** On February 14th, 2024, Trans-Northern Pipelines (TNPI), a major Canadian oil and gas pipeline operator, confirmed its internal network was breached in 2023. ALPHV/BlackCat claimed responsibility for the attack.[16]
- **Fidelity National Financial (FNF):** On January 9th, 2024, Fidelity National Financial confirmed in an SEC form 8-K filing that a cyberattack occurred on November 19, 2023, and confirmed hackers stole data on 1.3 million of its customers.[17] FNF said it was "contained" seven days later on November 26, 2023.[18] ALPHV/BlackCat claimed responsibility for the attack in a post on its dark web leak site.[19]
- **Norton Healthcare:** On December 8, 2023, Kentucky health system Norton Healthcare confirmed a ransomware attack in May 2023 that resulted in 2.3 million individuals' data being exposed in the attack.[20] The attack was claimed in May 2023 by ALPHV/BlackCat saying they allegedly stole 4.7TB of data from the healthcare system's compromised systems.[21]
- **Tipalti:** On December 4th, 2023, Tipalti, a major accounting software company, confirmed it was investigating a ransomware attack claimed by ALPHV/BlackCat targeting the company and its customers Roblox and Twitch.[22]
- **Henry Schein:** On October 15th, 2023, Henry Schein, a major healthcare provider confirmed it was "forced to take some systems offline"[23] to respond to a cyberattack that took place on October 14th. ALPHV/BlackCat added Henry Schein to its dark web leak site, saying it stole 35 terabytes of "sensitive data."[24]

References

[1] https://www.scmagazine.com/news/loandepot-confirms-ssns-leaked-in-breach-claimed-by-alphv-blackcat
[2] https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/0001831631/000183163124000004/ldi-20240104.htm
[3] https://www.scmagazine.com/news/loandepot-confirms-ssns-leaked-in-breach-claimed-by-alphv-blackcat
[4] https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/
[5] https://www.scmagazine.com/news/loandepot-confirms-ssns-leaked-in-breach-claimed-by-alphv-blackcat
[6] https://www.nytimes.com/2024/02/28/technology/biden-data-sales-china-russia.html#:~:text=President%20Biden%20will%20issue%20an,blackmail%2C%20scams%20or%20other%20harm.
[7] https://www.cpomagazine.com/cyber-security/russian-ransomware-gang-alphv-blackcat-resurfaces-with-300gb-of-stolen-us-military-documents/
[8] https://www.cpomagazine.com/cyber-security/russian-ransomware-gang-alphv-blackcat-resurfaces-with-300gb-of-stolen-us-military-documents/
[9] https://www.bleepingcomputer.com/news/security/fbi-cisa-warn-us-hospitals-of-targeted-blackcat-ransomware-attacks/
[10] https://www.cpomagazine.com/cyber-security/blackcat-ransomware-gang-recovers-from-early-december-law-enforcement-operation-restores-websites-seized-by-doj/
[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
[12] https://techcrunch.com/2024/02/26/ransomware-attack-change-healthcare-prescription-pharmacy-outages/
[13] https://www.reuters.com/technology/cybersecurity/cyber-security-outage-change-healthcare-continues-sixth-straight-day-2024-02-26/
[14] https://www.sec.gov/Archives/edgar/data/1137774/000119312524033753/d770643d8k.htm
[15] https://www.theregister.com/2024/02/19/alphv_claims_cyberattacks_on_prudential/
[16] https://www.bleepingcomputer.com/news/security/trans-northern-pipelines-investigating-alphv-ransomware-attack-claims/
[17] https://www.bleepingcomputer.com/news/security/fidelity-national-financial-hackers-stole-data-of-13-million-people/
[18] https://techcrunch.com/2024/01/09/fidelity-national-financial-data-breach/
[19] https://www.insurancebusinessmag.com/us/news/cyber/fidelity-national-financial-cyberattack--more-than-one-million-impacted-472531.aspx#:~:text=The%20cyberattack%20that%20hit%20FNF,its%20dark%20web%20leak%20site.
[20] https://apps.web.maine.gov/online/aeviewer/ME/40/0d29d7d3-48c2-4879-b6c7-32360396bd04.shtml
[21] https://www.databreaches.net/norton-healthcare-didnt-call-it-a-ransomware-attack-then-blackcat-claimed-responsibility-for-it/
[22] https://therecord.media/tipalti-alleged-ransomware-attack
[23] https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/
[24] https://cyware.com/news/healthcare-giant-henry-schein-hit-twice-by-blackcat-8457da45/