INFOSOURCES™

NEWSLETTER

They want what you've got. don't give it to them

June 2024

- Kaspersky uploaded classified documents, "then deleted them"
- Microsoft stops providing 50 cloud services to Russian companies
- All of Israel could be disrupted by a massive cyberattack
- Targeting European Officials Associated with Diplomatic Events in India, a New Backdoor
- Why are hackers targeting the health care industry more frequently?
- Overview of Russian Cyber Threat Groups APT28 and Sandworm.
- NATO Defines a Cyber Red Line in Relation to Russia Tensions.
- Survey onTicketmaster cyber incident.
- An attack by ransomware on England's health sector.
- Pharmaceutical giant Cencora says data was stolen in a cyberattack.
- Russian cybercriminals use Ubiquiti routers as a launchpad for covert operations.
- It might take months for UnitedHealth to fully recover from the hack.

CYBER-ESPIONAGE

Kaspersky uploaded classified documents, “then deleted them”

Kaspersky’s analysts were in possession of a cache of classified files belonging to the Equation Group, an extraordinarily powerful band of hackers that would later be exposed as an arm of the US National Security Agency.

Several reports alleged that Kaspersky’s popular anti-virus program uploaded powerful digital espionage tools belonging to the NSA and sent them to servers in Moscow and that the US learned that Kaspersky had acquired the NSA’s tools via an Israeli spying operation.

The New York Times, The Washington Post and The Wall Street Journal, all the three publications reported that someone at the NSA’s elite hacking unit lost control of some of the agency’s powerful surveillance tools after they brought their work home with them, leaving what should have been closely guarded code on a personal computer running Kaspersky’s anti-virus software.

But information security experts reading the bits of information dropped by anonymous government officials are still puzzling at whether Kaspersky is suspected of deliberately hunting for confidential data or was merely doing its job by sniffing out suspicious files.

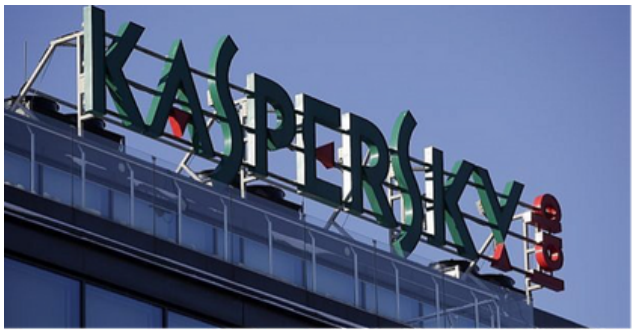
Much of the ambiguity is down to the nature of modern anti-virus software, which routinely submits rogue files back to company servers for analysis.

The software can easily be quietly tweaked to scoop up other files too: perhaps classified documents belonging to a foreign rival’s government, for example. Concerns have been fanned by increasingly explicit warnings from US government officials after tensions with Russia escalated in the wake of the 2016 presidential election.

Kaspersky denied any inappropriate link to the Russian government, and said in his interview that any classified documents inadvertently swept up by his software would be destroyed on discovery.

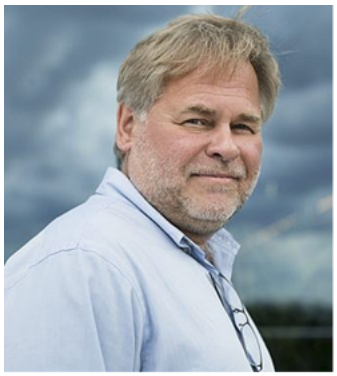
“If we see confidential or classified information, it will be immediately deleted and that was exactly (what happened in) this case,” he said, adding that the order had since been written into company policy.

Kaspersky’s account still has some gaps. How did the analysts know, for example, that the data was classified? And why not alert American authorities to what happened? Kaspersky declined to say whether he had ever alerted US authorities to the incident.



CYBER-ESPIONAGE

Jake Williams, a former NSA analyst and the founder of Augusta, Georgia-based Rendition InfoSec noted that Kaspersky was pitching itself at the time to government clients in the United States and may not have wanted the risk of having classified documents on its network. “It makes sense that they pulled those up and looked at the classification marking and then deleted them,” said Williams. “I can see where it’s so toxic you may not want it on your systems.”
As for the insinuation that someone at the NSA not only walked highly classified software out of the building but put it on a computer running a bootleg version of Office, Williams called it “absolutely wild.”



BLOCKING ACCESS

Microsoft stops providing 50 cloud services to Russian companies

Microsoft has suspended access to over fifty cloud products for Russian organizations as part of the sanctions requirements against the country issued by EU regulators last

December. The news of these impending suspensions was first reported by the Softline Group of Companies, one of Russia's largest remaining IT service providers.
Some of the most important products that will have their license keys invalidated are: Microsoft Azure, Dynamics 365, Microsoft Teams, Power BI, SQL Server, Visual Studio, Power Automate, SharePoint, Intune, Dynamics AX/NAV, Microsoft 365, OneDrive, Excel.
In addition to the above, Microsoft blocked access to LinkedIn-related software and the Media Player development kits. It has been clarified that the invalidation of licenses impacts Russian companies and organizations engaging in architecture, design, construction, manufacturing, media, education and entertainment, building information modeling (BIM), computer-aided design (CAD), and computer-aided manufacturing (CAM). Many Russian entities previously opted to purchase subscriptions to Microsoft products using foreign accounts or other bypasses.
The same fate is allegedly planned for Amazon, Google, and Oracle cloud services that fall under the same package of sanctions (2023/2873), with Russian users sharing an email on Telegram that they received from Amazon Web Services.

CYBERWARFARE

All of Israel could be disrupted by a massive cyberattack

Cybersecurity expert Refael Franco (founder and CEO of the cyber crisis management company Code Blue and former Deputy Head of the National Cyber Directorate) reveals the escalating cyber threats facing Israel. With daily attacks causing billions in economic damage, Franco warns of a potential catastrophic strike on critical infrastructure, highlighting the dangerous collaboration between Iranian and Russian cyber capabilities.

Since the beginning of the Iron Swords war, Israel has been grappling with a daily wave of thousands of cyber-attacks, primarily from pro-Palestinian and Iranian sources.
A report published about a month ago by Israel's National Cyber Directorate estimates the economic damage from these attacks at no less than 12 billion shekels per year.
About two weeks ago, the pharmaceutical company Rekah was forced to shut down its distribution system due to security breach concerns. Prior to that, a real estate website was disabled following a similar attack, and in an equally serious incident that occurred about a month ago, hackers breached the databases of the leading law firm Goldfarb Seligman.
Franco states, "Despite this improved recovery capability, Israel still faces a critical strategic vulnerability: the centralized management of our national infrastructure. How many 'Israel Electric Corporation' are there? How many 'Mekorot' [Israel's water company] companies are there? The country consists of a few companies that are the exclusive providers of strategic infrastructures."
"A massive cyberattack, one that disrupts the supply of electricity or water flow in Israel, is an event that can disrupt an entire country. If in the past Iranian efforts focused mainly on small and medium Israeli organizations with low levels of defense and awareness, in recent years Iran has been making enormous efforts to carry out a critical infrastructure attack against national companies," he claims.
"An event of this magnitude, if successful, could lead to a real disaster. Additionally, the Iranians understand very well how much of a moral blow this would be, causing enormous damage to the State of Israel and its citizens," Franco explains.
So far, attempts to damage infrastructure have not really succeeded, and the main impact has been on medium-sized organizations and below.
Although there has not yet been physical damage, the Iranians have managed to break into the systems of organizations of great importance, including medical institutions and academic institutions. They have managed to get their hands on a lot of information, which, although not strategic, is enough to cause economic damage to the economy.
While these recent attacks may appear to be of Palestinian origin,

they're actually being executed by Iranian operatives with Russian strategic guidance.

Russian support

Even before Tehran strengthened its strategic connection with Moscow, Iranian technology and research capabilities were considered relatively high, with the University of Tehran ranked among the top 500 universities in the world according to the Shanghai Index. Alongside these capabilities, the development in cyber in the last two years is a direct result of the strategic connection with Russia.

"In exchange for Tehran's unprecedented export of drones and weapons to Moscow, the Russians are enhancing and supporting Iranian cyber capabilities. This connection has developed the Iranian cyber array and led to its construction as an important and central factor in the campaign against Israel.

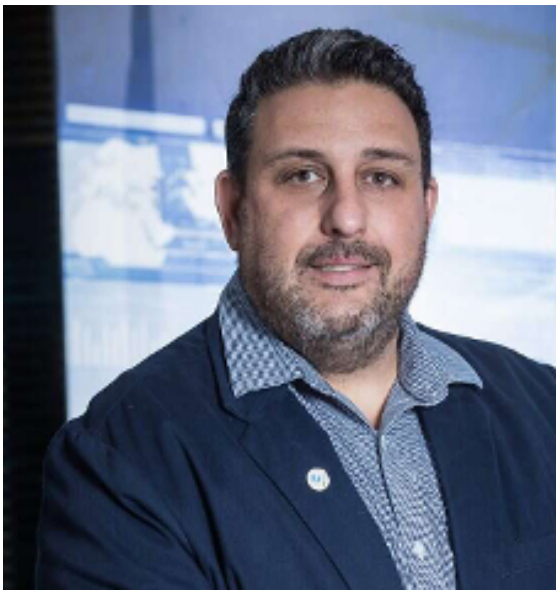
"The Russians, for their part, have long understood how critical psychological warfare and extensive use of fake news is in undermining enemy resilience, and the Iranians have adopted these tactics. Quite a few attacks make use of fake news and attempts to polarize Israeli public discourse."

Preparedness

The war has led the Israeli cyber industry to a boom it hasn't experienced for a long time, due to constant friction with attackers and the incorporation of Israeli creativity

The proof of this is the almost bi-weekly number of exits of Israeli cyber companies.

"However, the rapid advancement of Iranian cyber capabilities necessitates a shift in how we approach cybersecurity across our entire economy. A structured strategy, and consistent and clear guidelines through all bodies and factors in the Israeli economy, are critical to the continuous functioning of the State of Israel. Awareness of the threat, along with proper emergency preparedness that will allow rapid recovery from cyber-attacks, is what will make the chances of Iranians significantly harming Israeli society lower.



CYBERWARFARE

According to Microsoft, Russian hackers broke into company networks and obtained source code.

Midnight Blizzard, also known as NOBELIUM, APT29, and Cozy Bear, is a state-sponsored hacking group linked to Russia's Foreign Intelligence Service (SVR). This group recently gained access to Microsoft's internal systems and source code repositories by exploiting authentication secrets stolen during a January cyberattack. The breach involved accessing a legacy non-production test tenant account without multi-factor authentication, which was then used to infiltrate Microsoft's corporate environment. This account had access to an OAuth application with elevated permissions, allowing the hackers to access and steal data from corporate mailboxes, including those of Microsoft's leadership team and employees in the cybersecurity and legal departments.

Microsoft has indicated that Midnight Blizzard is now leveraging these stolen secrets, which likely include authentication tokens, API keys, or credentials, to gain further access to some of the company's systems and source code repositories.

The company is reaching out to affected customers to assist them in mitigating the risks.

Additionally, Midnight Blizzard is intensifying its password spray attacks. This type of brute force attack involves attempting to log into numerous accounts using a list of possible passwords until one succeeds.

Blizzard is infamous for its involvement in the 2020 SolarWinds supply chain attack, which compromised numerous companies, including Microsoft. The group also breached Microsoft again in June 2021, gaining access to customer support tools. Their cyberespionage activities have targeted NATO and EU countries, particularly embassies and government agencies. Apart from data theft, Midnight Blizzard is known for developing custom malware to support their attacks.

HEALTHCARE

Why are hackers targeting the health care industry more frequently?

Ransomeware A growing problem for hospitals

Ransomeware attacks in the US routinely force hospitals to divert ambulances and cancel appointments. That causes a strain on neighboring hospitals that pick up the slack. But a lack of clear public understanding of how cyberattacks on hospitals directly impact patient care is undercutting the urgency needed to deal with the problem, according to health advocates and cybersecurity experts. Researchers are increasingly quantifying how lethal ransomware can be. Roughly 3 in 100 hospitalized Medicare patients will die in the hospital under normal conditions, but during a ransomware attack, that number increases to 4 out of 100 because of the strain on hospital resources, according to scholars at the University of Minnesota School of Public Health, who studied 374 ransomware attacks on health providers. Part of the problem, experts say, is that some hospitals have failed basic tests of cybersecurity "hygiene," or sound defensive measures, while many small clinics lack the resources to secure themselves. And, perhaps more than any other sector, health care firms hold an enormous volume of sensitive data that is ripe for targeting and extortion schemes. The number of sensitive data records held by the health care sector grew by more than 63% last year "far surpassing any other industry and more than five times the global average," according to a study by security firm Rubrik. Health care providers also make attractive targets for cyber extortionists because hospitals can ill-afford to be offline for long because of the disruptions it causes to operations.

"When we look at ransomware targeting, it's: who is the most easily targetable, who can afford little downtime and who has the highest willingness to pay," "And where there's low-downtime environments, you have obviously a willingness to pay more so than in environments where they can afford downtime,"Bryan Vorndran, the FBI's senior most cyber-focused official, said in an interview.

Why are hackers targeting the health care industry more frequently?

Michigan Medicine estimated there are more than 500,000 hack attempts aimed at its systems daily.

,

About 60 to 80 attempts per month are “highly sophisticated.” Health care systems and their vendors have increasingly been the target of cyberattacks in recent years. When successful, these schemes can jeopardize patient personal information and cripple a hospital’s operations. Such was the case in May at Ascension, one of the nation’s largest health care systems. A worker accidentally downloaded a malicious file, allowing hackers to gain access to a “small number” of servers. Several hospitals in Michigan were left unable to access electronic health records and various systems to order tests, procedures and medications. Hospitals delayed some non-emergency elective procedures and, at times, diverted emergency medical services to other nearby care centers.

It could be months before the full damage of the attack is understood. Before then, another organization will likely find itself in a similar situation. Nationally, almost one in four ransomware complaints came from healthcare entities that year.

Why hospitals? It’s likely because of the massive databases of sensitive personal information they operate, and the importance of daily operations running smoothly. There’s a belief that because human lives are at stake, asking for ransom has a higher degree of likelihood they’ll get a very sizeable payout.

Hospital leaders are advised to be general with their explanations of attacks to avoid informing future hackers. Whether or not they pay a ransom is also often kept under wraps.

Hospitals rely on large databases of electronic medical records, not only for individual patient care. Researchers can analyze records for large populations to find rare complications for new medications and procedures, or to uncover a disease’s genetic/environmental contributors that may lead to new therapies. Great things result in massive, connected databases. If hackers gain access to patient information, they can use it for identity theft, credit card fraud, or to leverage sensitive information as blackmail for payment. That’s why it’s become common for businesses to offer free credit monitoring and identity theft protection services to patients and associates post-breech.

What hospitals are doing to defend themselves

Detecting who is behind an attack can be difficult, which makes prosecution frustratingly infrequent. Brian Peters, CEO of the Michigan Health & Hospital Association (MHA) said attacks can come from overseas and many are believed to be funded/backed by foreign states like China, Russia, North Korea and Iran.

In 2018, MHA teamed up with Beaumont Health, Munson Healthcare, and Michigan Medicine to create the Michigan Healthcare Security Operations Center. Information about new threats is routinely gathered by the group and shared with health systems around the state to help improve cybersecurity.

CYBERWARFARE

Overview of Russian Cyber Threat Groups APT28 and Sandworm

APT28, also known as Fancy Bear, is a Russian hacker group linked to the GRU, Russia's military intelligence agency. This group has been active since the early 2000s and is notorious for a series of high-profile cyber-attacks. Historically, APT28 has targeted organizations across the globe with sophisticated cyber espionage techniques. Notable incidents include the 2016 breaches of the Democratic National Committee (DNC) and the German Federal Parliament, which led to charges and sanctions against the group. Recently, APT28 has continued its activities through widespread phishing campaigns. These campaigns have utilized fake documents imitating government and non-governmental organizations from countries including Ukraine, Poland, and the U.S., to deploy advanced malware such as MASEPIE, OCEANMAP, and STEELHOOK for data exfiltration and system manipulation. The group's tactics also involve exploiting vulnerabilities like Microsoft Outlook's CVE-2023-23397 to perform relay attacks and exfiltrate NTLMv2 hashes.

Sandworm, another GRU-affiliated cyber threat group, is known for its aggressive and disruptive cyber operations. Since Russia's invasion of Ukraine, Sandworm has been actively involved in operations aimed at causing substantial disruptions to critical infrastructure. Their methods include the use of destructive malware like BlackEnergy and Industroyer to manipulate and disrupt utilities and other critical systems. Recent activities have included attacks on water utility systems in the US and Poland, as well as the manipulation of hydroelectric facility operations in France. Sandworm's operations are often synchronized with Russian military activities, aiming to achieve strategic objectives through visible and impactful cyber actions. In addition to these disruptive operations, Sandworm has been linked to the formation of APT44, which continues to conduct cyber-espionage activities and facilitate operations for Russian military interests, including a recent attack on the investigative journalism group Bellingcat.

Cyber Army of Russia, a hacktivist group linked to Sandworm, has engaged in a series of cyber sabotage operations. Although these efforts have involved minor disruptions, such as causing water level drops at facilities in Poland and the US, their impact has been limited. The group's activities are largely seen as propaganda efforts aimed at bolstering Russian domestic support for the war in Ukraine rather than achieving significant operational outcomes. Experts view the group's actions as more symbolic and aimed

CYBERWARFARE

at creating a perception of Russian cyber capabilities rather than executing effective sabotage.

In summary, while APT28 focuses on high-level espionage and data theft through sophisticated phishing schemes, Sandworm aims at direct disruptions of critical infrastructure to support military objectives.
Cyber Army of Russia serves as a more symbolic and propagandistic extension of Sandworm's activities. Together, these groups illustrate the range of tactics employed by Russian cyber actors from covert espionage to overt cyber sabotage.

APT28:
- Affiliation: Russian GRU.
- Known For: High-profile breaches (DNC, German Parliament).
- Recent Activities: Global phishing campaigns using fake documents; advanced malware (MASEPIE, OCEANMAP, STEELHOOK); exploitation of Microsoft Outlook vulnerabilities.

Sandworm:
- Affiliation: Russian GRU.
- Known For: Disruptive malware (BlackEnergy, Industroyer); attacks on Ukrainian infrastructure; manipulation of utilities in the US and Europe.
- Recent Developments: Linked to APT44; support for military operations; attack on Bellingcat.

Cyber Army of Russia:
- Affiliation: Linked to Sandworm.
- Known For: Cyber sabotage with minimal impact; symbolic acts to promote Russian interests.
- Recent Activities: Minor disruptions in water systems; propaganda efforts.

CYBER-ESPIONAGE

NATO Defines a Cyber Red Line in Relation to Russia Tensions

Recent developments in Russian cyber operations reveal a complex landscape of state-sponsored espionage and hacktivist activities aimed at both direct and indirect impacts on European political and critical infrastructure.

On May 3, 2024, the German government publicly condemned APT28, a notorious Russian hacker group linked to the GRU, for exploiting a Microsoft Outlook vulnerability to leak sensitive data from the SPD political party. This cyberattack, although categorized as cyberespionage, triggered a strong diplomatic response from Germany, including summoning the Russian ambassador and recalling its own envoy for discussions. The EU, NATO, the UK, and Czechia's Ministry of Foreign Affairs also condemned APT28's activities, which reflected broader concerns about Russian cyber tactics. While the specific incident involved espionage, the broader implications of such attacks are seen as part of Russia's strategy to interfere in elections and weaken democratic institutions.

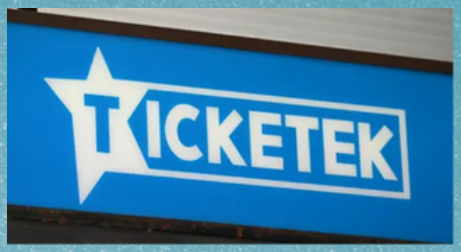
APT's recent activities align with their historical role in cyber-espionage, which includes notable breaches such as the 2016 attacks on the Democratic National Committee (DNC) and the German Federal Parliament. These attacks are often designed to influence political outcomes and gather intelligence that could be leveraged for broader strategic goals. John Hultquist, chief analyst at Mandiant Intelligence, emphasizes that while cyberespionage is a common statecraft tool, its use for election interference and its potential to disrupt democratic processes elevate it to a level of concern that approaches cyberwarfare. This interference aims to support pro-Russian political figures and destabilize Western alliances, thus contributing to a hybrid warfare strategy that combines

CYBER-ESPIONAGE

cyber operations with traditional military tactics.
In a related development, the pro-Russian hacktivist group NoName57(16) and other affiliated crews have recently threatened to launch cyberattacks on European internet infrastructure as the EU elections approach. This group, which emerged following Russia's invasion of Ukraine, has pledged to engage in Distributed Denial of Service (DDoS) attacks against European sites in retaliation for EU sanctions and perceived anti-Russian sentiments. Their planned cyber actions reflect a broader pattern of hacktivist efforts aimed at disrupting European democratic processes and critical infrastructure in response to international policies against Russia.

NoName57 and other hacktivist collectives like KillNet and Anonymous Russia have previously targeted Ukrainian sites and more recently shifted their focus to European targets. These groups are known for their DDoS attacks, which flood networks with malicious traffic, though their actual ability to cause significant damage remains limited compared to state-sponsored operations. Mandiant's analysts, including Hultquist, caution against overstating the impact of these hacktivist threats. While these attacks are designed to create uncertainty and draw attention to Russia's grievances, they are generally less capable of achieving substantive operational disruption compared to the more sophisticated and coordinated efforts of groups like APT28.
The interrelation between APT28's cyber-espionage efforts and the hacktivist activities of groups like NoName57(16) illustrates a strategic alignment within Russian cyber operations. APT28's intelligence-gathering serves to support longer-term strategic objectives, such as influencing political outcomes in Europe, while hacktivist groups engage in more immediate and visible acts of digital aggression to rally support for Russia's stance on international issues.
In summary, Russia's cyber activities encompass a spectrum of operations from high-level espionage to disruptive hacktivist campaigns. APT28 engages in sophisticated cyber-espionage to influence political processes and weaken NATO alliances, while NoName57(16) and similar groups conduct DDoS attacks as a form of cyber protest against European policies. These efforts reflect a broader hybrid warfare strategy that integrates cyber operations into Russia's geopolitical tactics, aiming to create division, weaken adversaries, and further Russian strategic interests.

CYBERCRIME



Survey onTicketmaster cyber incident

Ticketmaster is one of the premier booking and ticketing service providers for the arts and entertainment industry. It powers ticket sales for venues such as stadiums, performing arts centers, and museums, with a worldwide reach. By 2022, the company has become a global powerhouse and a de facto monopoly in ticketing events. Today, Ticketmaster controls the resale market, charging a service fee for tickets resold by private parties through its platform. Before the COVID-19 pandemic, the company was selling nearly half a billion tickets worldwide.

Industry publication CyberDaily reported that the personal details of 560 million Ticketmaster customers may have been leaked in a data breach claimed by a notorious hacker group Shiny Hunters. It said 1.3 terabytes of customer data possessed by Ticketmaster including names, addresses, credit card numbers, phone numbers and payment details is up for sale. Shiny Hunters may not have reportedly hacked Ticketmaster, and instead could effectively be serving as a middleman by selling the customer data, experts noted. The group's post said the data was available for purchase for $500,000 in a "one-time sale."

IT Experts said the hack will have major implications for Australian customers. "This could mean the potential risk of identity fraud and we would assume this data would be used for phishing or impersonation attacks down the track," experts said. "We should all be looking for multi-factor authentication and additional resources to protect ourselves".

Reports of the hacking come a week after Live Nation, which owns Ticketmaster, was sued by the US Department of Justice over claims it is running an illegal live event "monopoly". The DOJ alleged the ticketing giant's monopoly on the market was driving up prices for fans and pushing out smaller competition. The company said it distributed more than 620 million tickets in 2023.

Understanding the Hacking

A threat actor claiming recent Ticketmaster breaches says they stole data after hacking into an employee's account at cloud storage company Snowflake. However, Snowflake disputes these claims, saying recent breaches were caused by poorly secured customer accounts.

Snowflake's cloud data platform is used by 9,437 customers, including some of the largest companies worldwide, like Adobe, AT&T, Capital One, Doordash, HP, Instacart, JetBlue, Kraft Heinz, Mastercard, Micron, NBC Universal, Nielsen, Novartis, Okta, PepsiCo, Siemens, US Foods, Western Union, Yamaha, and many others. Security experts say that as more details become clear about hackers' attempts to access and take data

from Snowflake's systems, it is possible that other companies will reveal they had data stolen. At present, though, the developing situation is messy and complicated. According to cybersecurity firm Hudson Rock, the threat actor claimed they also gained access to data from other high-profile companies using Snowflake's cloud storage services, including Anheuser-Busch, State Farm, Mitsubishi, Progressive, Neiman Marcus, Allstate, and Advance Auto Parts.
However, Snowflake doesn't "believe" it was the source of any leaked customer credentials. "We have no evidence suggesting this activity was caused by any vulnerability, misconfiguration, or breach of Snowflake's product," Brade Jones, Snowflake CISO wrote in a blog post.

Bypassing Authentication

To do that, it is said attackers bypassed Okta's secure authentication process by signing into a Snowflake employee's ServiceNow account using stolen credentials. Next, they claim they could generate session tokens to exfiltrate data belonging to Snowflake customers. A single credential resulted in the exfiltration of potentially hundreds of companies that stored their data using Snowflake. The threat actor claims they wanted to blackmail Snowflake into buying back the stolen data for $20 million, but the company didn't reply to their extortion attempts.

The Hudson Rock post claimed that a Snowflake employee may have been infected by a Lumma-type infostealer that collected the details the hacker needed to log in to its systems. Charles Carmakal, the chief technology officer at Google-owned security firm Mandiant declared that its investigations, which have been taking place in recent weeks, indicate information-stealing malware may have been used to get Snowflake account credentials.

Countermeasures

Snowflake CISO Brad Jones notified all customers of the attacks and urged them to secure their accounts and data by enabling multi-factor authentication (MFA). The data cloud company also published a security bulletin with Indicators of Compromise (IoCs), investigative queries, and advice on how potentially affected customers can secure their accounts. One of the IOCs indicates that the threat actors created a custom tool named 'RapeFlake' to exfiltrate data from Snowflake's databases. Another one showed the threat actors connecting to databases using the DBeaver Ultimate data management tools, with logs showing client connections from the 'DBeaver_DBeaverUltimate' user agent.

Cloud security company Mitiga says its investigations have seen a threat actor targeting organizations using Snowflake databases

and using an attack tool called " rapeflake" in the process. Roei Sherman, field CTO at Mitiga, said, one possible scenario is that a threat actor managed to get information about Snowflake's systems and then stole information about its clients, possibly using automated tools and brute-forcing their way into accounts. Sherman added that the attack could have wider ramifications going forward. There are already early signs other companies may be impacted.

Ticketmaster Data Breach May Be Just the Beginning: Another Event ticketing company attacked

Cybersecurity researcher Kevin Beaumont shared online that he knows of six companies that have been impacted, among them the Australian events company Ticketek.
Ticketek is an Australian event ticketing company. Founded in 1990, the company is owned by TEG Pty Ltd with its headquarters in Sydney and operates ticketing operations for entertainment and sporting events in Australia and New Zealand. Ticketek sells around 18 million tickets to over 13,000 events annually. Ticketek was "a different company to Ticketmaster, which is a subsidiary of Live Nation Entertainment" – referring to the global hack of Ticketmaster. Ticketek has been hit by a "cyber incident" with personal information of Australian customers stolen from a third-party global cloud-based platform, Snowflake. The breach was "affecting many Australians" but appeared restricted to the release of names, dates of birth and email addresses. Passwords and credit card information have not been compromised. The breach is the second reported this week of a major global ticketing outlet. Ticketek emailed customers about the "cyber incident" affecting account holder information "stored in a cloud-based platform and reassure you that Ticketek has secure encryption methods in place for all passwords. In addition, secure encryption methods are used to handle credit card information and transactions are processed via a separate payment system, which has not been impacted.

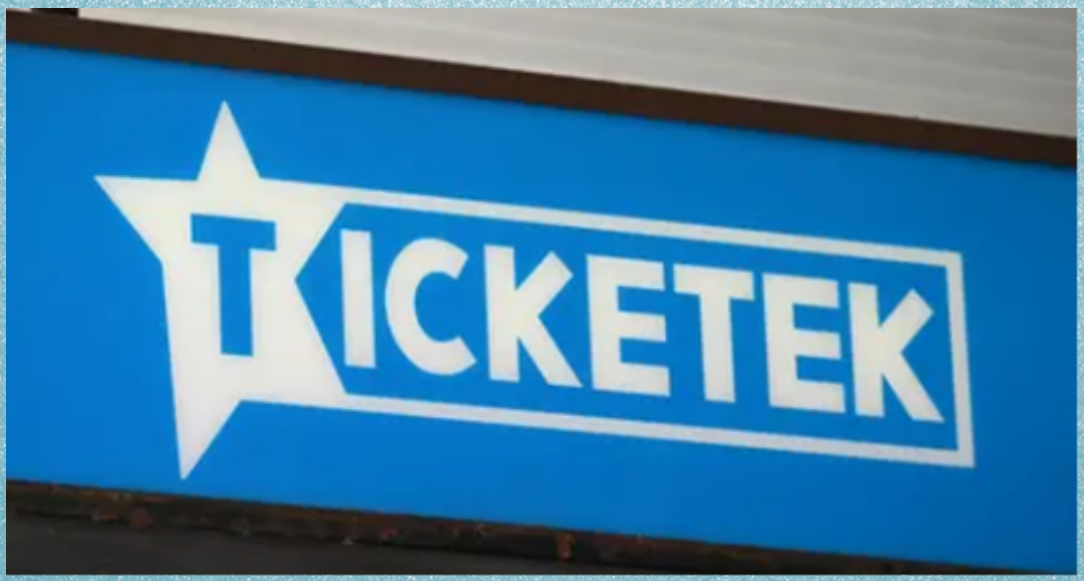
Notorious Shiny Hunters

The hacking group emerged in 2020 and drew attention the following year when it exposed huge troves of customer records from more than 60 companies, among them, selling 70 million AT&T records in 2021. For four years, Shiny Hunters stole 200 million customer records from more than a dozen companies when authorities caught up with Raoult. According to the Department of Justice, the Shiny Hunters stored and sold stolen data on the "dark web," including customer databases with personal and financial information. In fact, Shiny Hunters posted the exact same Ticketmaster ad on rival marketplace Breach Forums. On May 30, Shiny Hunters also claimed to be selling 30 million customer details
.

CYBERCRIME

and staff information from Santander, putting a $2 million price tag on the information. Both posts on Breach Forums have drawn attention to the illegal marketplace, which was recently revived by Shiny Hunters after the FBI took the website down on May 15. The posts may, at least in part, be efforts to restore the disrupted forum's damaged reputation with criminals. The two hacks were linked to Snowflake' s systems by Israeli security firm Hudson Rock, which, in a now-removed blog post, posted conversations its researchers had with the alleged hacker who claimed to have accessed Snowflake's systems and exfiltrated data. The hacker claimed they had tried to sell the data back to Snowflake for $20 million.

Sebastien Raoult, a French computer hacker and Shiny Hunters member, in January was sentenced to three years in prison and ordered to pay more than $5 million in restitution after pleading guilty to conspiracy to commit wire fraud and aggravated identity theft. In September last year, 193,000 Pizza Hut customers' data was leaked when Shiny Hunters allegedly accessed their personal information



RANSOMEWARE

An attack by ransomware on England's health sector

The National Health Service in England is urging people with universal blood types [O negative type] to donate after a ransomware attack disrupted hospitals' ability to match patients — underlining how cyberattacks can have serious and potentially life-threatening impacts.
On June 3, hackers targeted pathology services provider Synnovis with ransomware. Ransomware attacks encrypt a company's computer system, rendering it inoperable until the victim pays a fee. The attack on Synnovis severely impacted several London hospitals serving two million people, prompting them to declare a critical incident and cancel cancer surgeries and blood transfusions. Hospitals and other health-care providers are targeted by ransomware gangs because disruptions to life-saving treatments can increase the pressure to pay criminals, cybersecurity expert Steve Waterhouse said.
Hospitals across Canada have been targeted by ransomware gangs for years — a cyberattack last year impacted five hospitals in southwestern Ontario at once.
The effects of cyberattacks can be serious. A 2023 study by researchers at the University of Minnesota estimated that between 42 and 67 Medicare patients died as a result of delayed care due to ransomware attacks between 2016 and 2021.
The gang behind the NHS ransomware attack is suspected to be Qilin, a Russian-speaking entity. Ransomware groups like Qilin operate almost like startups, offering their software as a service to affiliates that carry out attacks. Many gangs are believed to operate in Russia, so they are likely to remain outside the reach of Western law enforcement.

Pharmaceutical giant Cencora says data was stolen in a cyberattack

Pharmaceutical giant Cencora, previously known as AmerisourceBergen, specializes in pharmaceutical services, providing drug distribution and solutions for doctor's offices, pharmacies, and animal healthcare. The Company had $262.2 billion in revenue for fiscal year 2023 and employs approximately 46,000 people. In a Form 8-K filing with the SEC, Cencora disclosed they suffered a cyberattack that led to data theft. Upon initial detection of the unauthorized activity, the company immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts, and external counsel. At this time, there is no further information on who breached Cencora and no ransomware gangs have taken responsibility. A ransomware group known as Lorenz previously claimed to have breached Cencora in February 2023 while the company was operating as AmerisourceBergen, stating that they stole data related to the Animal Health division.
The SEC filing is a financial statement or other formal document submitted to the U.S. Securities and Exchange Commission (SEC). Public companies, certain insiders, and broker-dealers are required to make regular SEC filings. Investors and financial professionals rely on these filings for information about companies they are evaluating for investment purposes.

CYBERWARFARE

Russian cybercriminals use Ubiquiti routers as a launchpad for covert operations

In recent years, a Russian advanced persistent threat (APT) group known as APT28, Fancy Bear, Forest Blizzard, or Pawn Storm, linked to Russia's Main Intelligence Directorate of the General Staff (GRU), has been leveraging a botnet primarily comprised of compromised Ubiquiti EdgeRouters. These routers, commonly found in small office/home office (SOHO) environments, were co-opted into a botnet used for various cyberespionage and cybercrime activities.

In January 2024, the US government, with support from international partners, successfully disrupted this botnet. The FBI reported copying and erasing stolen and malicious data from the affected devices and modifying firewall rules to block APT28's access. Despite these efforts, remnants of the botnet persisted due to the presence of undetected malware and additional compromised devices beyond the Ubiquiti routers.

Following the disruption, the US government urged organizations and consumers to cleanse their devices of Moobot malware, which played a crucial role in the initial compromise of the routers. This malware enabled APT28 to gain root access by exploiting default credentials and trojanized OpenSSH server processes, allowing extensive control over the devices.

Since 2016, cybercriminals began infecting Ubiquiti routers, and APT28 later gained access in 2022. These routers were used for various malicious purposes, including data collection, network traffic proxying, and hosting command-and-control infrastructure for the MasePie Python backdoor. The compromised devices facilitated espionage operations across Europe, the Middle East, and the US, and were involved in stealing webmail credentials, collecting NTLMv2 digests, and redirecting phishing traffic.

The botnet also involved additional malware such as SSHDoor, a backdoored SSH daemon for credential harvesting and maintaining persistent access, and Ngioweb malware, which is memory-resident and has been active since at least 2018. Custom scripts and routing rules supported phishing and other malicious campaigns by redirecting traffic and obfuscating the attackers' identities.

Despite the disruption efforts, Trend Micro reported that the cleanup operation did not fully eliminate the Russian hackers' access. The botnet included additional devices like Raspberry Pi and other Linux systems, along with over 350 compromised VPS IP addresses. Multiple threat actors, including the Canadian Pharmacy gang and groups using Ngioweb malware, also exploited the botnet.

The resilience of APT28 and the involvement of multiple threat actors highlight the complexity of the cyber threat landscape. These groups employ sophisticated anonymization techniques, using commercial VPN services and residential proxy networks to blend malicious activity with normal traffic. To mitigate these threats, organizations and consumers must thoroughly cleanse their devices, change default credentials, and ensure robust password policies. Regular monitoring and updating of devices are essential to patch vulnerabilities and detect abnormal activities early.

HEALTH CARE

It might take months for UnitedHealth to fully recover from the hack.

Health data is attractive to bad actors because it can be easily monetized and sold on the dark web to perpetuate other crimes like identity theft and health-care fraud, said John Riggi, national advisor for cybersecurity and risk at the American Hospital Association. He said there are different kinds of cyberattacks impacting the health-care sector, including data theft and ransomware attacks. In a data theft attack, bad actors sneak into a system and steal data. In a high-impact ransomware attack, the fallout can cause immediate harm to patients' physical safety. By encrypting all the data in networks, systems go dark, and data become unavailable . This means diagnostic technologies like CT scanners can go offline, and ambulances carrying patients are often diverted, which can delay lifesaving care.

UnitedHealth Group (UNH.N) is the biggest health-care company in the U.S. by market cap, and it owns the health-care provider Optum, which services more than 100 million patients in the U.S., according to its website. Change Healthcare offers tools for payment and revenue cycle management. Change processes about 50% of medical claims in the U.S. for around 900,000 physicians, 33,000 pharmacies, 5,500 hospitals and 600 laboratories. About 1 in 3 U.S. patient records are touched by its health technology offerings, making it an attractive target for hackers looking to gain access to a large swathe of healthcare data Change's system outages have disrupted operations in pharmacies and health systems across the country. Change Healthcare's systems are down after a cyber threat actor gained access to its network last week.

HEALTH CARE

Parent company UnitedHealth Group said most U.S. pharmacies have set up electronic workarounds to mitigate the impact. UnitedHealth discovered that a “suspected nation-state-associated” threat actor breached part of Change Healthcare’s information technology network. UnitedHealth isolated and disconnected the impacted systems “immediately upon detection” of the threat. Health care is a complex industry with lots of moving pieces and entry points, which means it can be hard for any organization to be 100% secure, said Cliff Steinhauer, director of information security and engagement at the National Cybersecurity Alliance.

UnitedHealth Group is likely to need several months to make a full recovery from a cyberattack that has been one of the most disruptive hacks against America's healthcare infrastructure, security experts said. The American Medical Association on Monday asked the Biden administration to make emergency funds available to physicians hurt by the outage.

Since its Change Healthcare unit was breached on Feb. 21 by a hacking group called ALPHV, also known as "BlackCat", UnitedHealth has said it is working to restore impacted channels, and that some of its systems are returning to normal. It said that they have been working with external partners like Palo Alto Networks to regain confidence.

UnitedHealth hasn't said if ALPHV demanded ransom, but a post on an online cybercrime forum claimed the company paid $22 million to the hackers for regaining access to its locked systems and around 8 terabytes, or 8 million megabytes, of data that was allegedly stolen, including information like medical records, insurance records and payment information. The ransomware gang claims that they stole source code for Change Healthcare solutions and sensitive information belonging to many partners, including the U.S. military's Tricare healthcare program, the Medicare federal health insurance program, CVS Caremark, MetLife, Health Net, and tens of other healthcare insurance providers. Such volume decryption can take “unreasonable amounts of time, depending on the file sizes and systems in question,” said Kurtis Minder, co-founder of cyber intelligence firm GroupSense. Minder, who has helped victimized organizations negotiate with ALPHV, said recovery timelines ranged from a few weeks to "long and longer." The post said a partner of Blackcat was responsible for the intrusion into UnitedHealth. The message, allegedly from the partner, included a link showing that someone had moved about 350 bitcoins, now worth about $23 million as the value of the cryptocurrency rises, from one digital currency wallet to another.

The owner or owners of the respective wallets is not publicly available, but blockchain analysis firm TRM Labs said the destination of the funds was "associated with AlphV," noting it had seen that address used to collect ransom payments from other AlphV victims. Brett Callow, a threat analyst at the cybersecurity company Emsisoft, said ransomware groups will often make posts like these in an effort to bring victims to the negotiating table.

REVENGE ATTACKS

The attack on Change Healthcare comes after 2023 set a grim record for health-related cybercrime. There were 725 large health-care security breaches last year, up from the record 720 the previous year, according to a January report from The HIPAA Journal. Months before ALPHV waged its most disruptive hack yet, it was hitting hospitals and small healthcare providers. Minder said he has helped several companies, including an eye care clinic that was an ALPHV target last year, negotiate with the hackers.
Active since at least 2021, the Russian-speaking ALPHV cybercrime gang provides its own malicious software and infrastructure to other hacking outfits, and was the world's second most prolific 'ransomware-as-a-service' entity until the FBI disrupted its operations in December. The FBI previously linked BlackCat to over 60 breaches during its first four months of activity (between November 2021 and March 2022) and said the gang raked in at least $300 million in ransoms from over 1,000 victims until September 2023.

For instance, breaches last year against were gambling firm MGM Resorts International (MGM.N) and consumer products company Clorox (CLX.N) impacted them for months, costing MGM at least $100 million in damages and Clorox a drop of more than $350 million in quarterly net sales. In response to the FBI takedown, ALPHV's administrator instructed its hacking 'affiliates' to target hospitals, according to a U.S. Cybersecurity and Infrastructure Security Agency (CISA) advisory about the group. There are some signs ALPHV may be quiet for a while. Following the Change Healthcare hack, the gang has pulled a disappearing act. But it is common for such groups to rebrand and resurrect themselves, analysts say.