Who is Cozy Bear and how can you protect yourself?

TeamPassword

August 24, 2021 · 10 min read Cybersecurity

Russian intelligence agencies have invested heavily in cyber espionage exploits over the past decade. One of those operations is the US classification, advanced persistent threat APT29—more commonly known as Cozy Bear.

Cozy Bear is a highly sophisticated Russian cyberespionage group focused on attacking US and NATO government institutions and multinational organizations.

NATO intelligence agencies, including the US, have evidence to believe Cozy Bear is a branch of the Russian Federal Security Service (FSB - formally the KGB) and possibly the SVR, another Russian intelligence agency.

How can you keep yourself safe from cybercriminals? TeamPassword helps small businesses prevent breaches with a secure password management tool to safely share login credentials with coworkers. Make sure you keep your passwords safe. Try our free trial by clicking here and seeing how it can work for yourself.

Who is Cozy Bear?

Leading Internet security firm Kaspersky Lab found that Cozy Bear's MiniDuke malware dates back to 2008 and that the group has targeted government organizations since around 2010.

It's unclear what "Cozy" refers to, but "Bear" is a codename for Russian hackers at security firm CrowdStrike.

Cozy Bear and Fancy Bear

On some occasions, Cozy Bear works with another Russian cyber espionage group, Fancy Bear (suspected as part of Russian military intelligence agency GRU). The latter is more infamous, but Cozy Bear is far more covert—possibly more dangerous than Fancy Bear.

The difference is that Fancy Bear appears to be a military operation, while Cozy Bear is a Russian central intelligence unit.

Where it's often clear that Fancy Bear is responsible for an attack, security firms and intelligence agencies can only speculate on most of Cozy Bear's most significant cyber operations.

Cozy Bear Aliases

Cozy Bear goes by many names given to them from security firms, intelligence agencies, and other organizations:

- APT29 - (Advanced Persistent Threat 29 - US federal government classification) most security firms and intelligence agencies use APT29 when referring to Cozy Bear
- CozyCar

- CozyDuke
- Dark Halo
- The Dukes
- Grizzly Steppe - for operations where Cozy Bear works with Fancy Bear
- NOBELIUM
- Office Monkeys
- StellarParticle
- UNC2452
- YTTRIUM

What does Cozy Bear do?

Cozy Bear's primary goal is to spy and gather intelligence on nations and multinational organizations. Cozy Bear dismantles or disrupts networks and infrastructure occasionally, but most of its operations appear to be gathering intelligence for Russia.

APT29's targets are primarily NATO allies; however, the group also spies on Russia's neighbors, including China, Ukraine, Uzbekistan, and other Transcaucasian nations.

The sophisticated cyberespionage group often breaches software, networks, and other IT systems where they lie hidden for extended periods spying and gathering intelligence.

Cozy Bear's toolset features an array of malware and trojans to infiltrate its targets, all likely designed by the group.

Cyber security analysts have commentated on how fast and efficient Cozy Bear is at developing and deploying its components—creating a substantial challenge for counter operations.

Famous Cozy Bear Attacks

Security firms and intelligence agencies suspect Cozy Bear of many large-scale cyber-espionage operations. But, due to the group's stealthy modus operandi, only a few attacks are directly attributed.

In some instances, US intelligence agencies also don't want to point fingers at Cozy Bear or Russia, as they don't want to reveal their "sources" or investigation methods.

Office Monkeys - 2014

Office Monkeys is one of Cozy Bear's first significant US operations where the group infiltrated and installed its trojan, CozyDuke, on a Washington D.C. research group's network.

The research group discovered the trojan in March, and shortly after, Cozy Bear began a spear-phishing campaign with an email attachment featuring office monkeys.

Victims who clicked the video inadvertently downloaded malware, giving Cozy Bear access to the device and any linked IT infrastructure—including many US government networks.

The group went about installing trojans on government networks. Needless to say, they caused countless disruptions in the process. They created a mess that took US authorities months to mop and fix.

At the same time, the Dutch General Intelligence and Security Service managed to infiltrate Cozy Bear's operations. The agency discovered APT29 was targeting the US Democratic Party, State Department, and White House.

The Pentagon - 2015

In 2015 Cozy Bear successfully breached the Pentagon's unclassified email system resulting in email shutdowns and disrupting Internet access.

Cozy Bear's 2015 Pentagon attack affected around 4,000 military and civilian personnel working for top-ranking US officials.

Democratic National Committee (DNC) - 2016

In a parallel hacking effort with Fancy Bear, Cozy Bear infiltrated the DNC in 2016, stealing user credentials and other data.

Fancy Bear's 2016 DNC operation was disruptive and destructive, while Cozy Bear seemed to gather intelligence in the shadows.

Later, investigators determined that Cozy Bear had access to the DNC's network for over a year while Fancy Bear had only gained access a few weeks before being detected.

The DNC operation leads intelligence agencies to conclude that Cozy Bear is a highly sophisticated, covert Russian espionage unit focused on a greater long-term objective.

Norwegian & Dutch Governments - 2017

In early 2017, Cozy Bear made multiple spear-phishing attempts to breach several Norwegian government departments and security agencies.

At the same time, the Cozy Bear and Fancy Bear targeted Dutch ministries to access secret government documents. It's unclear how Cozy Bear attempted these attacks, but it forced Holland to hand-count votes for the country's 2017 general elections.

COVID-19 Vaccine Data - 2020

In 2020, multiple US security agencies accused Cozy Bear of trying to steal vaccine and treatment data from US, UK, and Canadian organizations—likely to help Russia advance its vaccine program.

The group attempted to deploy custom malware known as *WellMess* and *WellMail* through various spear-phishing attacks.

SUNBURST Malware Supply Chain Attack - 2020

The SUNBURST attack was the catalyst for one of the biggest data breaches in 2020, the infamous SolarWinds attack impacting more than 18,000 businesses and governmental organizations.

In early December 2020, security firm FireEye discovered that hackers had stolen its cybersecurity research tools, resulting in one of the biggest supply chain attacks in history!

Some notable victims include:

- The Department of Homeland Security
- The Department of Energy
- The National Nuclear Security Administration
- The State Department
- Microsoft
- Cisco
- Deloitte
- Intel

The attackers caused havoc at Microsoft, stealing signing certificates allowing them to impersonate users and access accounts.

The Washington Post suggests its sources identify Cozy Bear as the culprits for the SUNBURST attack. Still, security firms and intelligence agencies say there isn't enough evidence to say for sure.

Security analysts suspect the SUNBURST attack involved several collaborative groups, each tasked with a different objective working towards a common goal—much like a coordinated military operation.

How Does Cozy Bear Attack Networks?

Cozy Bear deploys highly effective spear-phishing operations to breach its targets. These attacks usually require significant research, resources, and preparation to deploy successfully.

Cozy Duke's spear-phishing attacks are so sophisticated that they even manage to fool individuals with regular cyber security training—like governmental staff and software engineers.

Once Cozy Bear breaches a network, they try to remain undetected for as long as possible, gathering intelligence and stealthily installing custom malware.

How Can You Prevent an Attack from Cozy Bear?

The truth is Cozy Bear would probably hack most small businesses with relative ease. But the good news is it's highly unlikely Cozy Bear would even attempt to hack a small business—unless they're involved in any government contracts.

But that isn't to say there aren't hackers deploying similar spear-phishing attacks.

The best way to thwart breaches is by installing multiple security layers and, most importantly, educating employees about cybersecurity.

To breach a device or network, criminals must first install malware or steal an individual's login credentials. Hence the reason attackers deploy phishing tactics first.

Most cybercrime is a result of human error. Companies must plan for this by limiting access to systems and data and implementing a robust password management policy.

Password Management for Small Businesses

TeamPassword is an accredited secure provider utilizing state-of-the-art encryption technology for its password manager.

When you save new passwords, the data is hashed, salted, and encrypted locally on your computer before being uploaded to TeamPassword via an encrypted connection. This level of encryption makes it impossible for nefarious actors to intercept your passwords.

Built for Teams

You can share passwords securely with TeamPassword, and never have to provide employees or freelancers with raw login credentials.

Instead of sharing passwords for multiple applications, you provide team members with access to TeamPassword. Your team then uses one of TeamPassword's browser extensions (Chrome, Firefox, and Safari) to access your company or client accounts.

Essentially, TeamPassword works like a master key.

Create Groups & Limit Access

One way to minimize the impact of a breach is by limiting access to data and accounts. For example, if a freelancer is working on a client's Instagram account, they don't need access to the entire social media portfolio.

With TeamPassword, you can create groups for sharing passwords, limiting access to only those who need it. When a team member no longer needs access, you can remove them with one click.

Two-Factor Authentication

What if attackers steal an employee's TeamPassword login credentials?

TeamPassword features two-factor authentication (2FA) to provide your account with an extra layer of security. Without the user's mobile device for authentication, criminals can't get past the 2FA step, thus preventing a full breach.

Secure Unique Password Generator

Often cybercriminals don't need to breach a system—they can simply guess an easy password.

Some companies even reuse passwords for multiple accounts. If attackers manage to steal one password, they'll have access to all the accounts using the same credentials.

TeamPassword features a secure unique password generator to ensure your company never uses weak passwords or the same credentials for more than one account.

Sign up today for a free 14-day TeamPassword trial and protect your company's digital assets from cybercriminals.

Recommended Articles

Cybersecurity January 15, 2024 · 8 min read

Vishing: What you need to know to stay safe in 2024

Vishing is when hackers use the phone to get sensitive information from the recipient as part of a ...

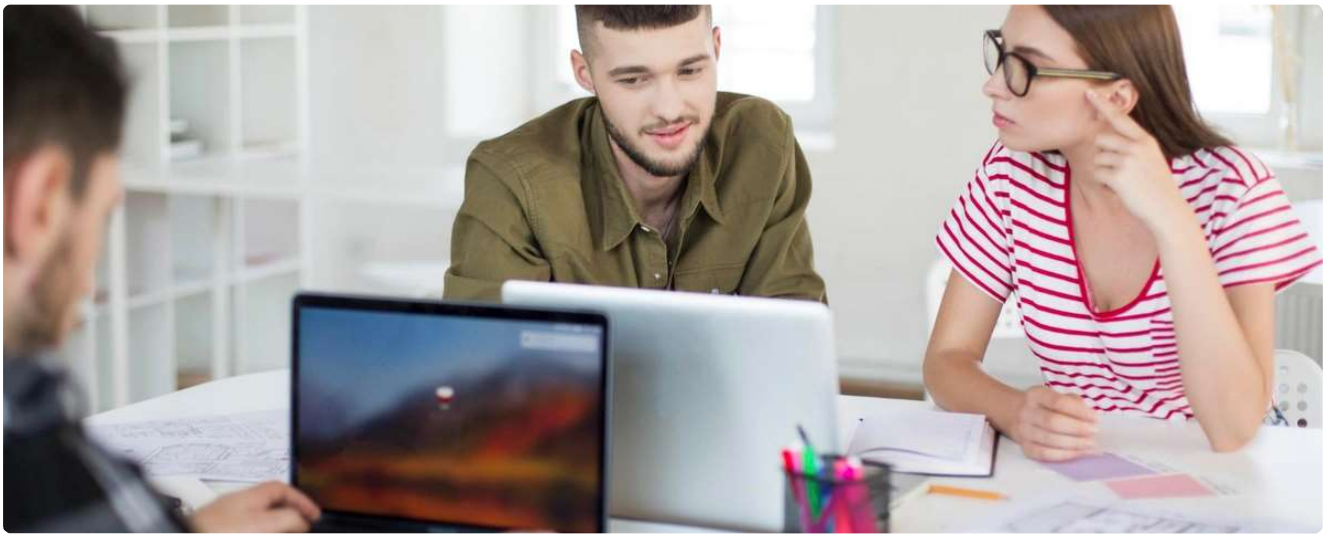
Timothy Ware

Cybersecurity December 6, 2023 · 11 min read

SME Cybersecurity | 5 Ways to Keep Your SME Secure

Small and medium-sized enterprises (SMEs) face a growing number of serious cybersecurity threats in the modern age, especially ...

Noah Bisceglia



Cybersecurity December 3, 2023 · 7 min read

8 Ways to Securely Manage Multiple Websites For Multiple Clients as an Agency

Explore 8 expert strategies for secure multi-website management as an agency. Elevate client satisfaction with robust security practices. ...

Tim Green

Product

Product Tour

Plans & Pricing

Password Generator

Customers

Support

Blog

Status

Support

Help

Channels

LinkedIn

Instagram

Facebook

Youtube

Legal

Security

Terms of Use

Privacy Policy