The Job Offer That Wasn’t: How We Stopped an Espionage Plot - SecurityScorecard

Archived: 2026-04-05 19:34:35 UTC

Discover how SecurityScorecard thwarted a sophisticated cyber-espionage plot disguised as a job offer. Learn about the 'Contagious Interview' campaign, the tactics used by the Famous Chollima group, and essential strategies to protect your organization from targeted attacks. Don't let your next career move become a trap—stay informed and secure!

In cybersecurity, transparency matters—because none of us are immune. Increasingly, we’re seeing threat actors hone in on specific organizations. When we detected the recent “Contagious Interview” campaign targeting one of our own, our team acted fast to stop it in its tracks. We’re sharing this story so others can see how easily these attacks unfold—and how quickly they need to be stopped to protect the community.

What if your next career move could be a trap? Imagine a job offer that seems perfect—right fit, right timing, and from a company you admire. But hidden behind that offer is a nation-state actor, ready to pull you into a cyber-espionage nightmare. That’s exactly what nearly happened to a SecurityScorecard developer in the “Contagious Interview” campaign.

SecurityScorecard is exposing a sophisticated phishing operation led by one of the world’s most dangerous threat groups: **Famous Chollima**. While they appeared to target intellectual property, their real aim may have been even bigger—stealing cryptocurrency. And they came alarmingly close to succeeding.

These attackers slip in unnoticed. They breach your systems. Before you even realize it, your data is gone and your assets are drained. It’s not just money at stake—your business grinds to a halt, data is lost, and trust is shattered. It’s the panic of knowing your systems are compromised, and everything is on the line.

Let’s walk through the intricate details of this incident, dissect the threat, and, more importantly, learn how to protect what matters most—your data, your people, and your business.

Looking for a detailed technical breakdown? Read the full analysis here

The “Contagious Interview” Campaign: What You Need to Know

The “Contagious Interview” campaign was a precision strike aimed at developers, engineers, and IT professionals, especially those working at tech startups. These attackers don’t cast a wide net; they pick their targets carefully.

Before making a move, they do their homework. They scour your social media, gathering every detail about you—your skills, connections, career goals—all to craft the perfect lure.

In this case, it all began with a LinkedIn message. On the surface, everything looked legitimate. A recruiter, offering what seemed like a dream opportunity: a role in a blockchain project. For a developer interested in crypto, it was the kind of offer that's hard to pass up. What the developer didn't know was that the recruiter's profile had been compromised by attackers.

The developer was specifically targeted based on public LinkedIn data and their involvement in a crypto-related Telegram group. The attackers knew exactly who they were dealing with—what the developer did, what they were interested in, and how to bait the hook just right.

How the Attack Unfolded: An Engineer's Worst Nightmare

Initial Contact via LinkedIn:

A message popped up. A well-known tech company was scouting blockchain experts. The offer was enticing—too good to pass up. The recruiter provided a link to a coding challenge, describing it as part of the technical interview process.

To move forward, they provided a link to a coding assessment, supposedly part of the technical interview process. The developer, eager to advance their career in the crypto space, saw this as an opportunity too good to miss. So, they clicked.

The Trap:

The coding test looked innocent enough—just a code review hosted on Bitbucket. But the Bitbucket account was controlled by the attackers. Hidden in the code was *BeaverTail*, a Remote Access Trojan (RAT) linked to Famous Chollima. So when the developer cloned the code to their GitHub account from their corporate device—a serious breach of company policy—the malware silently deployed.

BeaverTail went to work immediately, attempting to download a second malware, *InvisibleFerret*. This second-stage malware would have given the attackers deep access to the developer's corporate device. So, the company's defenses stepped in.The security team acted fast, stopping the malware before it could deliver the full blow.

Threat Actor Attribution: Famous Chollima

Famous Chollima, a cyber-espionage group tied to North Korea is fueling a regime. North Korea's hackers target cryptocurrency to evade international sanctions, funneling billions into the country's nuclear weapons program. By infiltrating tech companies and financial platforms through spear-phishing and custom malware, they transform stolen digital assets into untraceable funds, strengthening one of the world's most isolated and dangerous regimes. Each attack is a direct investment in global instability, with every stolen coin fueling a growing threat.

In this campaign, Famous Chollima once again proved their skill at exploiting public data sources like LinkedIn and Telegram. By gathering detailed information about their target, they crafted communications so personalized

and convincing that even a seasoned professional fell for the bait.

STRIKE Team: Swift, Decisive, and Effective

As the attack unfolded, SecurityScorecard's STRIKE Team noticed unusual activity on the developer's device. The STRIKE Team didn't hesitate—they moved fast, isolating the threat before it could dig deeper into the network.

The STRIKE Team approached the attack with years of training and expertise. Every move was calculated, drawing on years of experience and a deep understanding of how these threats unfold. The attackers, making their own moves, tried to spread malware, disrupt the network, and capture valuable data.

But the team anticipated their every step.

They secured systems, cut off infiltration points, and blocked the paths the attackers could take. Each action was deliberate, countering the enemy's strategy with precision and skill.

The attackers sought chaos, but the STRIKE Team responded with control.

In the final move, the team isolated the malware before it could spread, shutting down the attackers' game entirely. What could have been a disaster was neutralized almost as soon as it began—the attackers never stood a chance.

While not every detail of their incident response playbook can be disclosed, the core principles remain: isolate, contain, and neutralize. In this case, the success of the response was in the speed, coordination, and preparation of the team.

In this case—and as part of our ongoing commitment to transparency in the Infosec community—the SSC STRIKE Team shares critical intelligence with the FBI to disrupt threat actor's operations. This approach reflects our broader strategy to partner regularly with law enforcement, strengthening defense efforts across the board.

To prevent a breach like this from happening, security teams must reinforce every link in the chain—from employee training to system safeguards. Flexibility in defense strategies and anticipating the attackers' next move is critical when dealing with threat actors as skilled as Famous Chollima.

Whether you're building your team's capabilities through internal training or calling in expert help, your defenses need to be ready for anything.

Understanding the Malware: BeaverTail and InvisibleFerret

BeaverTail Malware:

BeaverTail is a lightweight Remote Access Trojan (RAT) designed to give attackers full control over a compromised machine. Once it's running, it can log keystrokes, capture screenshots, and steal stored credentials. In this case, *BeaverTail* was delivered through trojanized NodeJS code, cleverly hidden within what seemed to be a legitimate coding challenge. Its role was to silently execute and lay the groundwork for further infiltration.

InvisibleFerret Malware:

InvisibleFerret is a more advanced second-stage payload that Famous Chollima often uses in attacks like these. If successfully installed, it provides long-term persistence, making it much harder to detect and remove. It's also equipped for lateral movement, allowing the attackers to spread through the network and escalate the breach. In this incident, *InvisibleFerret* was blocked before it could fully deploy, but had it succeeded, the damage could have been far worse.

Our defenses stopped this threat, and we're sharing our lessons to help you stay safe. Cyber threats are relentless, but you don't have to face them alone. When stakes are high, SecurityScorecard's STRIKE Team is ready to protect your business—because every second counts.

Lessons Learned and Best Practices: How to Protect Against These Attacks

1. **Limit Public Information Sharing:**
   Developers and other high-value employees need to be careful about what they share online. Attackers often piece together profiles from LinkedIn and similar platforms to customize their phishing attacks. Limiting publicly available information can reduce your exposure to targeted campaigns.
2. **Security Awareness Training:**
   Companies should continually refresh their security awareness programs to include phishing and job-based social engineering scenarios. Employees need to be taught how to spot and verify unsolicited job offers or interview requests, especially when these involve unfamiliar downloads or links.
3. **Customized Endpoint Security:**
   EDR tools are effective, but they must be tuned to detect real threats in your specific environment. Alerts should not be dismissed as routine without proper investigation. Visibility into endpoint traffic and forensic capabilities are critical for understanding the attacker's tactics and stopping them before they can escalate.
4. **Corporate Device Policies:**
   Strict policies regarding corporate device usage are essential. Personal activities should never be conducted on company devices, especially when interacting with unknown or untrusted contacts online. Using non-approved software on corporate systems opens the door to potential security risks.
5. **Credential Management:**
   Enforce the use of multi-factor authentication (MFA) and apply strict credential management policies. Credentials should be rotated regularly, particularly for employees working on sensitive projects or accessing cloud services. This adds a layer of defense against potential breaches.

Final Thoughts

The "Contagious Interview" campaign is a reminder that even the smallest click can open the door to a major breach. It's like being handed a red pill from *The Matrix*—once you're in, there's no turning back. This attack wasn't just a one-off event; it shows how attackers exploit trust and ambition to slip into the most secure environments.

For businesses, it's time to adopt a zero-trust mindset. Verify everything—every device, every user—before it's too late. The real takeaway? Stay a step ahead. Train your people, lock down your systems, and don't rely on hope

to defend your network.

Want to ensure your organization stays safe and ahead of threats? Don’t leave security to chance. Contact the experts at SecurityScorecard today and together we’ll keep your company secure.

Good luck and stay vigilant!
Steve Cobb
