WHITEPAPER

Cyber Risk Intelligence: Idaho National Laboratory Data Breach

SecurityScorecard

SecurityScorecard.com

info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

Executive Summary

- On November 20, a spokesperson for Idaho National Laboratory (INL) confirmed that it had suffered a data breach.
- The confirmation followed the SiegedSec threat actor group's circulation of claims that it had "accessed hundreds of thousands of user, employee and citizen data" on social media and hacking forums.
- Findings from both SecurityScorecard's internal at-risk credential collections and a strategic partner's NetFlow data may suggest that INL experienced activity resembling tactics, techniques, and procedures (TTPs) SiegedSec used in the previous incidents discussed above.
- The following IP addresses may be particularly likely to have been involved in SiegedSec's activity:
  - 198.54.128[.]115
  - 198.54.128[.]20
  - 165.232.128[.]166
  - 198.54.129[.]102
  - 192.42.116[.]15
  - 192.42.116[.]185
  - 98.159.33[.]36
- SecurityScorecard therefore recommends that organizations monitor their networks for communication with them and consider adding them to firewall and endpoint blocklists.

Background

On November 20, a spokesperson for Idaho National Laboratory (INL) confirmed that it had suffered a data breach that exposed the personal data of INL employees and other users of its Oracle human capital management (HCM) system. The confirmation followed the SiegedSec threat actor group's circulation of claims that it had "accessed hundreds of thousands of user, employee and citizen data" on social media and hacking forums.

Prior to the INL breach, SiegedSec most recently attracted attention when, shortly after the outbreak of the current conflict in Gaza, the group claimed that it would, alongside the pro-Russian hacktivist group Anonymous Sudan, target critical infrastructure in Israel in a series of apparently unsuccessful denial-of-service (DoS) attack attempts. However, the INL incident resembles SiegedSec's earlier activity (which often revolved around the circulation of stolen data) more than it does the group's claimed attempts against Israeli industrial control system (ICS) devices.

In late July 2023, SiegedSec published a collection of files it purportedly stole from NATO's portal for sharing unclassified information. In late June, it claimed a series of breaches of U.S. state and local government agencies, which some officials described as relatively low-impact, noting that they did not appear to have exposed sensitive information. Earlier, in February of this year, the group claimed to have attacked Atlassian and published employee and office data. Atlassian's investigation of the incident concluded that SiegedSec accessed the data by using leaked employee credentials to authenticate to Envoy, a third-party application Atlassian used.

Findings from both SecurityScorecard's internal at-risk credential collections and a strategic partner's NetFlow data may suggest that INL experienced activity resembling tactics, techniques, and procedures (TTPs) SiegedSec used in the previous incidents discussed above.

Findings

The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team consulted SecurityScorecard's internal datasets, a strategic partner's NetFlow data, and publicly-available information to develop further insight into the incident.

SecurityScorecard's leaked credential collections contain twenty-nine unique records for subdomains of inl[.]gov and two records for INL's Taleo subdomain, inl.taleo[.]net. None of usernames for inl[.]gov subdomains feature @inl[.]gov email addresses, and the specific subdomains suggest that they correspond to (possibly externally-facing) training sites, and may therefore offer few insights into SiegedSec's access to INL's Oracle HCM system. The exposed login to INL's Taleo subdomain may offer some insights.

INL's statement confirming the breach points out that attackers compromised INL's Oracle HCM (human capital management) system. Because Oracle owns Taleo (which is an HCM tool), this record may contain credentials for the system targeted in the incident. Even if SiegedSec did not use the particular credentials contained in SecurityScorecard's collections in the attack, they could reflect a wider effort to distribute information-stealing malware ("stealers") to INL personnel.

SecurityScorecard's at-risk credential collections come from stealer logs, which threat actors (possibly including SiegedSec, but also including ransomware groups) use to steal login information which they then can reuse (or sell for other actors to reuse) to access and compromise target systems. The appearance of an INL Taleo account in those logs indicates that at least one INL employee or applicant's device was infected with a stealer and may further suggest that the other INL employees or applicants' devices may have suffered similar infections.

Reusing compromised credentials is a fairly common way for threat actors in general to access target systems, and one SiegedSec in particular has used in the past, as in the Atlassian breach discussed above. The Atlassian incident is additionally similar to the INL incident as in both cases, SiegedSec accessed the affected organizations' data by leveraging exposed credentials for third-party services (Envoy in Atlassian's case, and Oracle HCM in INL's).

The NetFlow samples the STRIKE Team collected may additionally offer some evidence of traffic resembling SiegedSec activity. A collection of the same IP addresses identified as proxies communicated with an IP address to which inl.taleo[.]net recently resolved and with different IP addresses attributed to INL. This may reflect SiegedSec's behavior: the group has boasted that they do not fear law enforcement because they are "behind 7 proxies," an apparent reference to a long-standing meme. While identifying these IP addresses may not help identify the individuals responsible for SiegedSec's operations, it may assist in defending against them: possible target organizations should monitor their networks for evidence of communication with them.

Of the IP addresses that the partner providing the traffic samples linked to virtual private networks (VPNs) or proxy services, the following may be particularly likely to have been involved in SiegedSec's activity, as they appeared in both the INL traffic samples involving and traffic samples collected in response to previous SiegedSec-claimed breaches. The strategic partner that provides SecurityScorecard's NetFlow data has, moreover, linked them to VPNs or other proxies. This, alongside their recurrence across multiple different SiegedSec targets' traffic samples, may suggest that SiegedSec used them.

- 198.54.128[.]115
- 198.54.128[.]20
- 165.232.128[.]166
- 198.54.129[.]102
- 192.42.116[.]15
- 192.42.116[.]185
- 98.159.33[.]36

Conclusion

Although the INL breach does not appear to have compromised the laboratory's most sensitive data, the exposure of information regarding its personnel is nonetheless cause for concern, as threat actors could base future targeting upon the data exposed. Given that social engineering may have been a feature of the activity leading up to the breach—and that activity exploiting the data exposed as a result of it could also revolve around social engineering—taking steps to defend against social engineering may reduce the risk of future similar incidents and limit the impact of the recent breach. To safeguard against social-engineering, organizations should engage in increased security awareness training, use multi-factor authentication, and closely monitor possibly-exposed credentials.

About SecurityScorecard

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company’s robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard.com
info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

SecurityScorecard