NOCTURNUS | THREAT ALERTS

BITBUCKET MALWARE ARSENAL

OVERVIEW

THREAT TYPE:
MULTI-PAYLOAD ATTACK

TARGET INDUSTRY:
ACROSS ALL INDUSTRIES

ATTACK GOAL:
STEAL SENSITIVE DATA
& SPREAD RANSOMWARE

IMPACTED GEO:
ACROSS ALL GEOS

REMEDIATION STEPS

Reimage any affected machines because of the different persistence mechanisms used.

Change all passwords related to affected services, both browser-based and local applications.

EXPERIENCED A BREACH?
EMAIL US AT

INFO@CYBEREASON.COM

WHAT'S HAPPENING?

The Cybereason team is following an active campaign to deliver multiple different types of malware and infect victims all over the world. Due to the viariety of malware types deployed in this attack, the attackers are able to steal a wide array of sensitive data, mine for Monero, and in certain cases also deploy ransomware. All of the payloads observed in this campaign originated from a code repository platform, Bitbucket, which was abused as part of the attackers delivery infrastructure.

KEY OBSERVATIONS & TTPS

- Attacks from all sides: This campaign deploys an arsenal of malware for a multi-pronged assault on businesses. It is able to steal sensitive browser data, cookies, email client data, system information, and two-factor authentication software data, along with cryptocurrency from digital wallets. It is also able to take pictures using the camera, take screenshots, mine Monero, and in certain cases also deploy ransomware.
- **Far Reaching:**
  This ongoing campaign has infected over 500,000 machines worldwide thus far.
- Cybereason reached out to Bitbucket Support and the malicious repositories mentioned in the report were deactivated within a few hours.
- **Read the full length research** here.

CYBEREASON CUSTOMERS

PREVENTED & DETECTED BY
THE CYBEREASON DEFENSE PLATFORM

We highly recommend every customer enable the following features:

- Monitor authorized access to Bitbucket repositories.
- If you do not have Cybereason NGAV activated, consider doing so to prevent against threats like these.
- **For Cybereason MDR customers, the Cybereason team will monitor and triage as well as assist in the mitigation of potential infections.**