kindred

Security Newsletter

10 February 2020

Subscribe to this newsletter

Bitbucket cloud Abused to Infect 500,000+ Hosts with Malware Cocktail

Attackers are abusing the Bitbucket code hosting service to store seven types of malware threats used in an ongoing campaign that has already claimed more than 500,000 business computers across the world. Systems falling victim to this attack would get infected with multiple payloads that steal data, mine for cryptocurrency, and culminate with delivering STOP ransomware.

According to research Cybereason published today, the targets are users looking for cracked versions of commercial software, "Adobe Photoshop, Microsoft Office, and others." The bait programs include Azorult and Predator the Thief infostealers, with the former collecting the data it was built to loot and the latter establishing a connection to Bitbucket to funnel in more malware.

Exhausting all money-making opportunities from a compromised host is a practice cybercriminals have exercised for a long time. Information can be sold on underground forums, cryptocurrency wallets can be depleted, and miners can mint digital coins. When there is nothing to steal from the infected system, attackers deploy ransomware for one last attempt to make a profit. In this case, however, STOP ransomware can also download other malware, prolonging the compromise. Attribution, as in many cases, is a difficult proposition, but the team continues to actively track the operators. Cybereason reached out to Bitbucket with the firm's findings and the company is investigating.

Read More on ZDNet

Even More on BleepingComputer

Coronavirus “safety measures” email is a phishing scam

Sadly, cybercrooks love a crisis, because it gives them a believable reason to contact you with a phishing scam. Fortunately, at least for fluent speakers of English, the criminals have made numerous spelling and grammatical mistakes that act as warning signs that this is not what it seems.

Never let yourself feel pressured into clicking a link in an email. Most importantly, don’t act on advice you didn’t ask for and weren’t expecting. If you are genuinely seeking advice about the coronavirus, do your own research and make your own choice about where to look.

Don’t be taken in by the sender’s name. This scam says it’s from “World Health Organization”, but the sender can put any name they like in the From: field. If you realise you just revealed your password to imposters, change it as soon as you can. The crooks who run phishing sites typically try out stolen passwords immediately (this process can often be done automatically), so the sooner you react, the more likely you will beat them to it. Never use the same password on more than one site and turn on two-factor authentication (2FA) if you can.

Read More on NakedSecurity

More #News

- Magecart group jumps from Olympic ticket website to new wave of e-commerce shops
- NIST Drafts Guidelines for Coping With Ransomware
- PayPal SMS scams – don’t fall for them!
- Google Accidentally Shared Private Videos of Some Users With Others
- Google launches open-source security key project, OpenSK
- Tech Support Scam Hitting Microsoft Edge Start Page Takes a Break
- Ashley Madison breach victims have more to worry about
- NSA Security Awareness Posters

- How to change iOS 13 settings for better security
- Am I a target?
- Google to block some HTTP file downloads starting with Chrome 83

#Patch Time!

- Sudo Bug Lets Non-Privileged Linux and macOS Users Run Commands as Root
- Chrome 80 Released With 56 Security Fixes, Cookie Changes, More
- Critical Android flaws patched in February bulletin
- 5 High Impact Flaws Affect Cisco Routers, Switches, IP Phones and Cameras
- Researcher Finds Over 60 Vulnerabilities in Physical Security Systems
- Cisco Patches Critical CDP Flaws Affecting Millions of Devices
- Vulnerability in WhatsApp Desktop Exposed User Files
- Medtronic Releases Patches for Cardiac Device Flaws Disclosed in 2018, 2019
- Trend Micro Patches More Vulnerabilities in Anti-Threat Toolkit
- Flaw in Philips Smart Light Bulbs Exposes Your WiFi Network to Hackers
- Critical Android Bluetooth Flaw Exploitable without User Interaction

#Tech and #Tools

- TUF: A framework for securing software update systems
- Improving email security with MTA-STS
- Analyzing WhatsApp Calls with Wireshark, radare2 and Frida
- Polyshell: A Bash/Batch/PowerShell polyglot
- Understanding CVSS v3.1
- Dufflebag: Uncovering Secrets in Exposed EBS Volumes
- Codict: Source Code Assessment and Programming references,Learning Framework
- CSP (Content Security policy) evaluator
- OK Google: bypass the authentication!
- Introducing Conditional Access for the Office 365 suite!
- Uncoder.io: SIGMA to SIEM Query translator
- Red Team Operations guide
- Move faster, Stay longer
- End-of-life announcement for CoreOS Container Linux
- CDP0wn: 5 0-days vulnerabilities in Cisco Discoveries Protocol
- Sysmon Community Guide Released
- Elemental - An ATT&CK Threat Library
- Using Office 365 Activity API and Power BI for security analysis (Part 1)
- Red Team Blues: A 10 step security program for Windows Active Directory environments

Kindred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us