CYBERMINUTE
Alberta Cybersecurity Insights
Alberta

TLP: WHITE

BlackCat: Leak Site Seized and Retaliation

In mid-December 2023, the BlackCat/ ALPHV ransomware gang's leak site went down and speculation was that it had been seized by law enforcement; a thought that was confirmed by the US Department of Justice on December 19th. Several international law enforcement partners collaborated on this take down, including agencies from Australia, Austria, Denmark, Germany, Spain, Switzerland, the UK, and the USA. The seizure not only saw access to BlackCat's primary leak site removed but also access to several of their other communication sites. Another benefit coming out of this seizure was the development of a novel decryption tool. Hundreds of BlackCat's victims were provided the tool by law enforcement, saving them from having to pay a ransom to regain control of their systems.

Unfortunately, within hours of the announcement by the Department of Justice, BlackCat posted claims that they had regained control of their leak site and as a form of retaliation removed some of their self-imposed rules. Prior to this take down, BlackCat had sectors that they refused to allow their ransomware to target, such as critical infrastructure, hospitals, and nuclear power plants; however, now they are saying none of these are off the table and they are actively encouraging other hacking groups to use their ransomware to hit US critical infrastructure.

Another move being touted by BlackCat and another ransomware group LockBit, in the wake of the seizure, is a push towards ransomware gangs forming cartels to better protect themselves from the efforts of law enforcement.

This past year has seen a distinct evolution of ransomware tactics and the fallout of this take down is seeming to herald another shift as 2024 starts. Preventative and detective measures—such as keeping systems up to date with the latest patches and fixes, monitoring potential vulnerabilities, reviewing audit logs for abnormalities, and ensuring multi-factor authentication methods are employed—are good ways to help protect against potential ransomware attacks.

Click Here to Read More!

Nova Scotia to Investigate MOVEit Data Breach

The impacts of the MOVEit data breach in June 2023 are still being felt as we enter the new year, with at least 2,662 organizations and 83 million people affected by the breach. One of the first major victims that came forward in June was the province of Nova Scotia, and at the beginning of December 2023, they announced that their provincial Information and Privacy Commissioner would be looking into the attack as part of a larger investigation into data theft in the healthcare sector. The focus of the investigation is stated to be a review of the security and incident response practices of the province’s healthcare sector.

Over the past several years, the healthcare sector has consistently set new records for the number of organizations affected by cyber threats, and 2024 appears poised to continue this alarming trend. This trend underscores the critical need for members of this sector to emulate Nova Scotia’s proactive stance in reviewing and enhancing their practices for preventing and responding to cyber threats. In late 2023, the Cybersecurity & Infrastructure Security Agency (CISA) released specific guidance for health-related organizations in preventing ransomware, emphasizing how common a target they are becoming.

With legislation relating to cybersecurity and critical infrastructure being tabled in the House of Commons and with the impacts being felt in the health sector, some experts are wondering if healthcare should be added to the list of critical infrastructure sectors being targeted by the Bill. If passed, Bill C-26 would see the chosen sectors be held legally responsible for developing, implementing, and maintaining a functioning cybersecurity program. This program would have to include mitigations against supply chain attacks—such as the attack that resulted from the MOVEit breach. All cyber incidents would also

12-year-old Bug Discovered in Bluetooth Protocol Impacts the Majority of iOS, Android, and Linux Devices

In August of 2023, bug-hunter Marc Newlin conveyed the details of a 12-year-old vulnerability to Google, Apple, and Canonical. On December 6th-8th, this vulnerability was publicly disclosed as CVE-2023-45866. The source of this exploit lies in the Bluetooth protocol and the manufacturer implementation of this protocol. This vulnerability enables an attacker to remotely inject unauthenticated keystrokes into an in-range target device. A successful exploit could allow an attacker to install malware, read and record messages, run arbitrary commands, and so on. The attack works by tricking the target device into pairing—without user confirmation—with an attacker-controlled Bluetooth keyboard. It is the remote equivalent of an attacker plugging a malicious USB into your device.

The iOS, macOS, Android, and Linux devices vulnerable under varying circumstances are listed in the original post. Notably, Android devices are vulnerable simply by having Bluetooth enabled. Vulnerable platform versions include those listed in the National Vulnerability Database (NVD). On December 11th, Apple addressed the issue with iOS patch 17.2, and macOS patch 14.2; all earlier versions of iOS are vulnerable. Google released patches for Android version 11-14, however, there is no security fix for versions 4.2.2-10. Several Linux distributions have security patches which were released in 2020 that remedy this vulnerability, but these fixes are disabled by default.

A threat actor does not need specialized hardware to successfully perform this attack, and a full proof of concept will be officially released on January 12-14th at the ShmooCon hacker conference.

have to be reported to the federal government, as per this proposed legislation.

Click Here to Read More!

Thus, Android, Linux, and Apple users should ensure their devices are up to date prior to this release date. Further, it would be good practice to disable Bluetooth when it is not being actively used. Vulnerabilities such as this one can cause major headaches for organizations who manage their employees' devices. Should a managed device become compromised—from this vulnerability or any other—it could result in a loss of confidentiality, integrity, and availability, or be the beginning of an enterprise-wide ransomware attack.

Click Here to Read More!