Cyber Awakeness Month: Takedown of Trigona, Hive Ransomware Resurges, RansomedForum and New RaaS ‘qBit’

Published: 2023-10-23 · Archived: 2026-04-05 16:51:19 UTC

From the takedown of Trigona to the resurgence of Hive Ransomware, and the emergence of a new hackers’ hub, significant events have recently transpired in the ransomware ecosystem.

In the ongoing cyber battle, it is imperative to stay well-informed about the latest ransomware incidents to fortify your cybersecurity defenses.

This blog post will provide a quick and informative overview of these recent ransomware events, offering a fresh perspective on the ransomware threat landscape.

Trigona Ransomware: Hacked and Defaced

The Ukrainian Cyber Alliance (UCA) detected a vulnerability in the Trigona gang’s Confluence server and promptly seized the opportunity to hack their servers. They meticulously copied all available information before wiping the servers clean.

This initial breach enabled UCA to access other Trigona-run sites, where they acquired copies of internal chats, data, and even the website’s source code. Subsequently, they defaced Trigona’s TOR negotiation and data leak sites.

Trigona’s website has been defaced

Trigona Ransomware publicly acknowledged the breach on a hacker forum, announcing their intentions to launch new sites by the end of **October 22**.

Trigona acknowledging the breach (Source: X)

BlackCat Deploys Munchkin ISO for Stealth

The BlackCat/ALPHV ransomware operation now deploys **“Munchkin,”** a tool that uses virtual machines for stealthy network device encryption. Munchkin allows remote system operation and network share encryption.

Palo Alto Networks Unit 42 discovered that Munchkin is a custom Alpine OS Linux distribution provided as an ISO file. After compromising a device, the threat actors create a new virtual machine using the Munchkin ISO, which comprises a set of scripts to facilitate password dumping, lateral movement, executing programs and deploying the BlackCat encryptor.

How does BlackCat utilize the Munchkin tool? (Source: Palo Alto Networks)

RagnarLocker’s Site Has Been Taken Down by Law Enforcement

In a concurrent development, the **RagnarLocker** data leak and negotiation sites displayed a seizure banner. As part of a coordinated international law enforcement operation, authorities apprehended a malware developer associated with the RagnarLocker ransomware gang and successfully seized control of the group's dark web sites.

RagnarLocker's data leak site has been seized (Source: BleepingComputer)

WeedSec Drops Moodle Databases

In a startling incident, the threat actor group "WeedSec" posted sample databases of **moodle[.]org** on its Telegram channel. Moodle is an online learning and course management platform, used by schools, universities, colleges, vocational trainers, and workplaces alike.

The leaked data in their initial share includes **moodle.sql (3GB)** and **erpnext.sql (1.1GB)**, followed by an archive share.

WeedSec leaks Moodle databases

Emergence of Hunters International: Potential Rebranding of Hive

Following the FBI's takedown of Hive ransomware, the operators have transitioned to a fresh endeavor named "Hunters International."

According to Rivitna on X, the sample employed by Hunters International is **Hive v6**. BushidoToken revealed there are numerous code overlaps and remarkable similarities that firmly connect Hive with this new venture.

The researchers' findings suggest a potential evolution or rebranding of the Hive ransomware operation.

Results of an analysis on Intezer (Source: X)

RansomedVC Launches a New Hub for Threat Actors: RansomedForum

The cybersecurity community has recently observed the emergence of a new cybercrime forum, established by the novel ransomware operation, RansomedVC.

The forum, named **RansomedForum**, serves as RansomedVC's primary leak blog and provides a platform for cybercriminals. In their welcoming message to fellow threat actors, RansomedVC detailed the forum's existing features and those in development, addressing anticipated questions from potential members.

RansomedForum can rapidly evolve into a central hub for threat actors seeking to exchange information, tools, and tactics related to ransomware attacks, potentially contributing to an increase in ransomware threats.

RansomedVC's announcement on RansomedForum (Source: X)

Fresh RaaS in the Cybercrime Market: Introducing qBit, the New Ransomware

The emergence of the new hacker forum has quickly given rise to a new threat within the cybersecurity landscape. A new ransomware variant named **qBit** has swiftly made its debut on the RansomedForum, with a post shared by

the user “qBitSupp.”

This ransomware is currently in its Beta stage, qBitSupp claims it is built from scratch using Go, making it a fresh addition to the ransomware scene. qBit operates on a Ransomware as a Service (RaaS) model, offering many features.

Features of the qBit ransomware

The threat actor behind qBit advertises that it has faster encryption speed, a low detection rate, and remarkable versatility. It is worth noting that there are both Windows and Linux variants available, tested on various builds. The threat actor also mentions the development of an **ESXi version** and lists additional features designed to enhance its malicious capabilities.

qBit aims to be an affordable and accessible choice, making it attractive for newcomers to the world of cybercrime. According to a recent message from qBitSupp, they provide their affiliates with an 85/15 profit-sharing arrangement:

qBitSupp’s statement about the payment structure

The threat actor has even shared demo videos, providing an unsettling glimpse into the potential harm this ransomware can inflict. This new development adds to the growing concerns within the cybersecurity community, highlighting the proliferating nature of ransomware threats.

Stay Updated on New Ransomware Threats with SOCRadar

In a world where the ransomware landscape is in a constant state of flux, staying informed is your best defense. Cybercriminals adapt swiftly, and so must our defenses.

With SOCRadar **Dark Web News**, you stay updated on the latest threats and trends emerging within the threat actors’ communities, enabling you to proactively safeguard your assets and organization.

SOCRadar Dark Web News

Furthermore, SOCRadar’s Threat Actor & Malware tracking feature furnishes you with detailed insights into these threats, including current and new ransomware threats.

SOCRadar Threat Actors/Malware page – BlackCat (ALPHV) Ransomware

Empowering yourself with knowledge represents the primary step in fortifying your digital realm. Confronted with ever-changing ransomware threats, ongoing vigilance, proactive defense, and real-time threat intelligence access can significantly enhance your cybersecurity posture.
