HC3: Analyst Note

January 28, 2022 TLP: WHITE Report: 202201281300

Cyber Threat Posed by BlackMatter RaaS Reduced to Guarded (Blue)

Executive Summary

The following report provides updated information regarding the BlackMatter ransomware-as-a-service (RaaS) program. While HC3 previously identified multiple healthcare and public health (HPH) sector or health sector-affiliated organizations impacted by this malware, the group has not claimed a victim since October 31, 2021 and appears to have shut down operations. HC3 is reducing the threat level posed by BlackMatter to BLUE or GUARDED.

Report

Previously, on September 2, 2021, the Health Sector Cybersecurity Coordination Center (HC3) issued a threat briefing titled "Demystifying BlackMatter" in which we provided information on what the BlackMatter RaaS operators claim to be and what we know about the group as well as technical details and mitigations for the ransomware variant. At that time, HC3 considered this threat a highly sophisticated, financially-motivated cybercriminal operation that posed an elevated risk to the healthcare and public health (HPH) sector despite the group's claims to not target healthcare entities. While no HPH victims were observed at that time, the group's suspected predecessors (DarkSide and REvil) had previously claimed health sector victims. BlackMatter is a Russian-speaking threat group likely originating from Eastern Europe which emerged in July 2021. The group's suspected predecessors were responsible for several high-profile incidents, including the Colonial Pipeline and Kaseya VSA attacks.

On October 18, CISA, FBI, and NSA issued a joint Cybersecurity Advisory (AA21-291A) providing information on BlackMatter ransomware. The advisory stated that BlackMatter is a possible rebrand of DarkSide and noted that the cyber actors have demanded ransom payments ranging from USD $80,000 to $15,000,000. The alert provided technical details with tactics, techniques, and procedures (TTPs) obtained from a sample of BlackMatter ransomware. Detection signatures, mitigations, and other resources were also provided.

The BlackMatter RaaS stated from its inception that the group was seeking to obtain network access to corporations in the US, Canada, Australia, and the UK with revenues of over USD $100 million. Even though the average revenue calculated for the 36 victims observed to date is about USD $231 million, many of the victim organizations which appeared on the leak site have a far lower revenue than the actor's initial target revenue. In fact, nearly 60% of the victims observed on the leak site have a company revenue of less than USD $100 million, with nearly 20% of total victims possessing a revenue of less than USD $10 million. HC3 has also observed victims in countries not included in the group's initial desired target geography. Approximately 50% of victims were based in the United States.

HC3 is aware of at least four healthcare or healthcare-related organizations which have been impacted by BlackMatter ransomware incidents. The US-based organizations include a pharmaceutical consulting company, a medical testing & diagnostics company, and a dermatology clinic. A global medical technology company based in the Asia-Pacific region also suffered a BlackMatter incident. Additionally, the BlackMatter RaaS operators claimed a U.S.-based law firm providing COVID-19-related legal services as a victim. The most recent BlackMatter victim was observed by HC3 on October 31. On November 1, BlackMatter claimed it was shutting down operations following pressure from local law enforcement and stated that key members of its group were "no longer available." Shortly thereafter, the existing BlackMatter victims were moved to the competing LockBit ransomware negotiation site.

Analyst Comment

HC3 assesses that the current cyber threat posed to the US HPH sector by the BlackMatter RaaS operators is BLUE or GUARDED, reduced from a previous assessment of Elevated (Yellow) in September 2021. HC3 can confirm that the BlackMatter leak site is no longer operational and no known ransomware variants are believed to be successors at this time, according to open source reporting. While the group appears to have shut down operations, other actors seeking lucrative payouts from ransomware attacks are likely to fill this void.

Appendix A: Victim Industry Analysis

The chart below presents a summary of the victim industries impacted by BlackMatter ransomware to date. This data was sourced from the BlackMatter ransomware blog, open source news reports, and information shared with HC3 from trusted third parties. The industry with the most victims was the food and beverage sector. There were at least four healthcare or healthcare-related entities (denoted by red bar) which either appeared on the BlackMatter blog or reported BlackMatter ransomware incidents. The U.S.-based dermatology clinic and a global medical technology company were both impacted by BlackMatter on or around September 8, 2021. The management consulting company dedicated to the pharmaceutical industry appeared on the BlackMatter blog on October 6, 2021 and the medical testing company appeared on September 17, 2021.

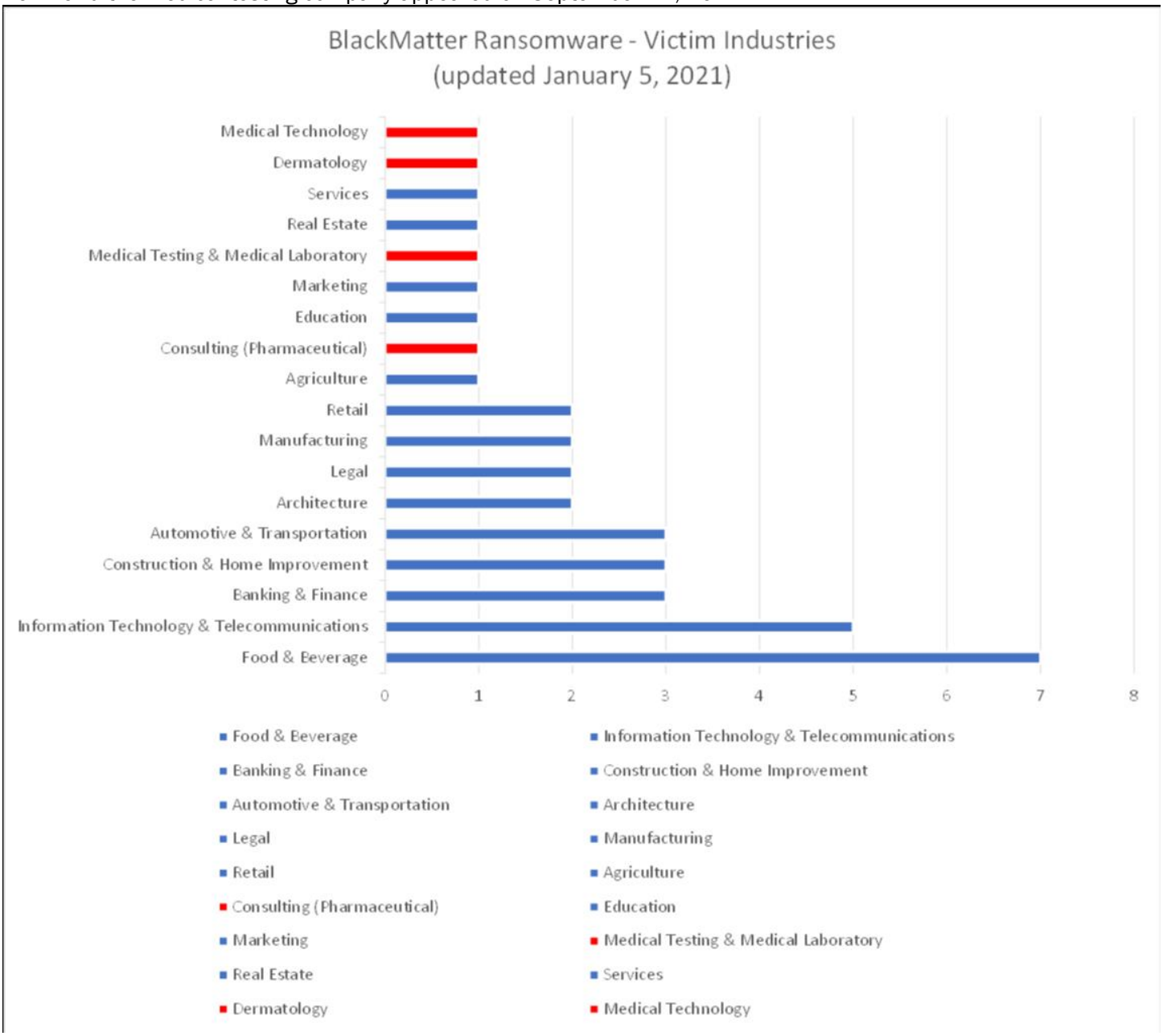

Figure 1. BlackMatter Victim Industries. Source: HC3

Appendix B: Timeline of Activity

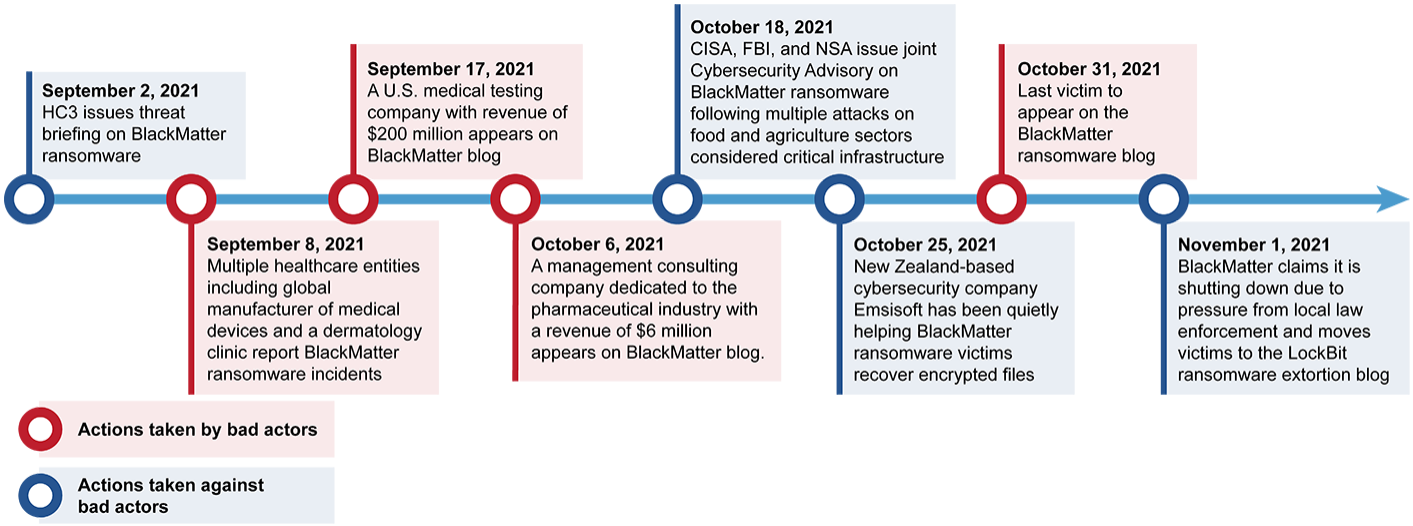

Figure 2. Timeline of activity related to BlackMatter. Source: HC3

References

CISA. "Alert (AA21-291A) BlackMatter Ransomware" 18 October 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-291a

Flashpoint, "Chatter Indicates BlackMatter as REvil Successor," 27 July 2021. https://www.flashpointintel.com/blog/chatter-indicates-blackmatter-as-revil-successor/

Naraine, Ryan. "DarkSide Ransomware Shutdown: An Exit Scam or Running for Hills?," 14 May 2021. https://www.securityweek.com/darkside-ransomware-shutdown-exit-scam-or-running-hills

Abrams, Lawrence. "BlackMatter ransomware gang rises from the ashes of DarkSide, Revil," BleepingComputer. 31 July 2021. https://www.bleepingcomputer.com/news/security/blackmatterransomware-gang-rises-from-the-ashes-of-darkside-revil/

Fisher, Dennis. "BlackMatter Ransomware Group Claims It's Shutting Down," 3 November 2021. https://duo.com/decipher/blackmatter-ransomware-group-claim-its-shutting-down

Abrams, Lawrence. "BlackMatter ransomware moves victims to LockBit after shutdown," 3 November 2021. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

Page, Carly. "A coding bug helped researchers build a secret BlackMatter ransomware decryption tool," 25 October 2021. https://techcrunch.com/2021/10/25/blackmatter-ransomware-bug-decryption-tool/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback