HC3: Threat Profile

March 15, 2023 TLP:CLEAR Report: 202303151200

Threat Profile: Black Basta

Executive Summary

Black Basta was initially spotted in early 2022, known for its double extortion attack, the Russian-speaking group not only executes ransomware, but also exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it, should a victim fail to pay a ransom. The threat group's prolific targeting of at least 20 victims in its first two weeks of operation indicates that it is experienced in ransomware and has a steady source of initial access. The level of sophistication by its proficient ransomware operators, and reluctance to recruit or advertise on Dark Web forums, supports why many suspect the nascent Black Basta may even be a rebrand of the Russian-speaking RaaS threat group Conti, or also linked to other Russian-speaking cyber threat groups. Previous HC3 Analyst Notes on Conti and BlackMatter even reinforce the similar tactics, techniques, and procedures (TTPs) shared with Black Basta. Nevertheless, as ransomware attacks continue to increase, this Threat Profile highlights the emerging group and its seasoned cybercriminals and provides best practices to lower risks of being victimized.

Impact to HPH Sector

Having already attacked several health and public health sector organizations in 2022, Black Basta is a credible threat to the sector. In its first year alone, the group exclusively targeted U.S.-based organizations, seeking to purchase network access credentials for companies specifically located there. In these attacks, Black Basta not only affected the websites of specific health information technology, healthcare industry services, laboratory and pharmaceutical, and health plans organizations across multiple states, but also cumulatively stole several gigabytes of data on personal identifiable information (PII) for members of health organizations, their customers, and employees. Continued and future attacks on and unpatched critical vulnerabilities in the public health and healthcare systems sector could be potentially life threatening, the impact of which would be devasting to critical infrastructure.

Figure 1: Sample Black Basta Ransomware Note. *(Trend Micro Incorporated – Ransomware Spotlight: Black Basta)*

Overview

Although Black Basta was first observed in April 2022, evidence suggests that the RaaS threat group was in development since February 2022. In its first two weeks alone, at least 20 victims were posted to its leak site, a Tor site known as *Basta News*. It exclusively targets large organizations in the construction and manufacturing industries, but was also observed to target other critical infrastructure, including the health and public health sector. While primarily targeting organizations within the United States, its operators also expressed interest in attacking other English-speaking countries' organizations in Australia, Canada, New Zealand, and the United Kingdom. Threat actors that used the ransomware have additionally impacted organizations based in the United States, Germany, Switzerland, Italy, France, and the Netherlands.

The highly capable and succesful organization has kept a closed profile over the last year, indicating that it may be similar to private groups like Conti, TA505, and Evil Corp. Rather than rely on comprehensive spray-and-prey tactics, the elusive group takes various precautions and relies on a more targeted approach, calculatingly assessing its victims before compromise. The group either excludes affiliates or only collaborates with a limited and trusted set of affiliates. Regardless, in only a short span of time, by

remaining under the radar, Black Basta has conducted massive breaches in critical instrastructure across multiple countries.

Nomenclature and Associations/Affiliations

For purposes of this product, Black Basta is identified as a unique RaaS group and ransomware. However, similar tactics, techniques, and procedures (TTPs) with other Russian-speaking threat actors suggest the idea among many that Black Basta is closely related to or has current and former operators from other groups, like Conti, FIN7, and/or BlackMatter. The possible connection to these groups could explain the high level of sophistication behind Black Basta's recent activity.

Motivations

Like most cybercriminals, Black Basta is primarily financially motivated. As in most ransomware incidents, the group sometimes even demands a ransom fee that exceeds millions of dollars. Operators in the group have expressed interest in specifically targeting English-speaking ("Five Eyes") countries, which could suggest a possible political agenda.

Common Tactics, Techniques, and Procedures (TTPs)

Black Basta operators are cunning, often utilizing unique TTPs to gain entry, spread laterally, exfilrate data, and drop ransomware. The ransomware is a cross-platform ransomware that is only executed with administrator privileges on both Windows and Linux systems. The ransomware hinders machine processes and ultimately makes desktop files unusable before sending a ransom note to a victim. Their previous attacks suggest that they use stolen credentials (purchased on the Dark Web) to get into organizations' systems. Initial access is often acquired via malicious links in a phishing e-mail. Unlike most cyber threat actors, Black Basta uses numerous tools and remote access methods. Common tools utilized by the group include Qakbot (aka QBot), SystemBC, Mimikatz, ColbaltStrike, and Rclone.

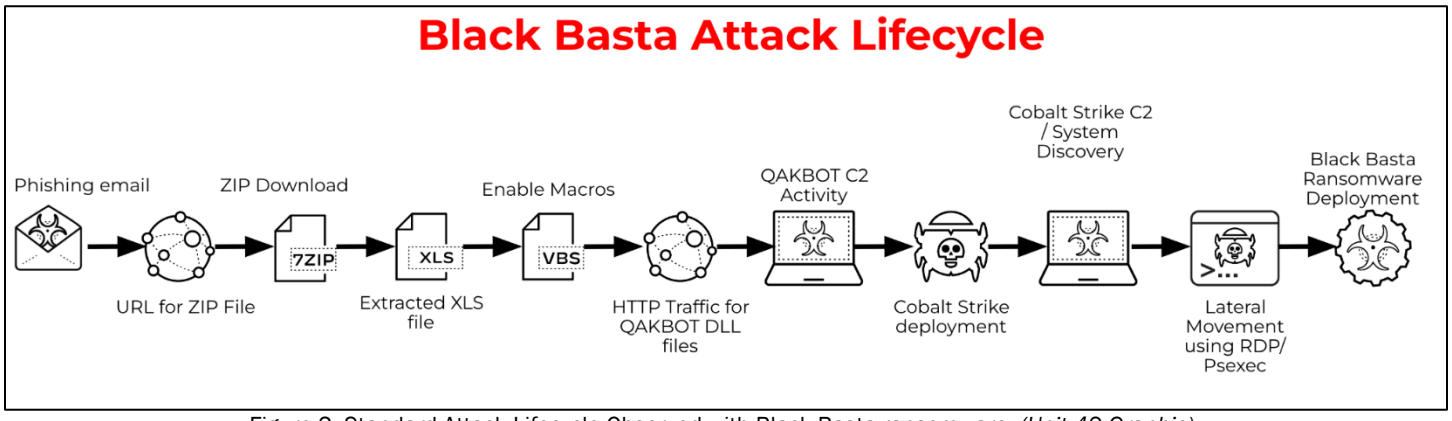

Figure 2: Standard Attack Lifecycle Observed with Black Basta ransomware. *(Unit 42 Graphic)*

It then deploys a name-and-shame approach to their victims, using a Tor site, *Basta News,* to publicly list victims' names, descriptions, percentage of published data stolen, number of visits, and any other data exfilrated. The data leak site, itself, can be found at the following Tor address (stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion/). Once the encryption process is complete, the malware changes the wallpaper, and files on the desktop become encrypted and unusable.

Observed Black Basta attack vector TTPs include insecure and vulnerable remote desktop protocol (RDP)

configuration, phishing campaigns, malicious downloads, web injections, and repackaged or infected installer. Unit 42 has also observed Black Basta affiliates utilizing the following TTPs. A list of the TTPs used by the group mapped against the MITRE ATT&CK framework can additionally be found here.

Relationships

Conti

Owing to a successful first few months of successful and coordinated attacks, speculation persists that Black Basta may be an offshoot of the Russian-speaking RaaS threat group, Conti, or has some members of the formerly proficient group. Conti utilizes RaaS to deploy disruptive ransomware attacks that target critical infrastructure, especially on the health and public health sector. The group prioritizes targeting companies with more than $100 million in annual revenue. They also specialize in double extoration operations, blackmailing their victims by threatening to publish stolen data.

Specifically, observers on the Dark Web note similarities between the two groups' data leak site infrastructures, payment methods, and communication styles. In addition, previously leaked Conti chats in February 2022 indicated that Conti operators may have tried to evade law enforcement by rebranding and working under a new ransomware group. Many noted that the leak of Conti's internal chats and source code would mitigate or even capitulate the group's previously successful ransomware campaigns. Subsequently, however, the group simply started to rebrand and strategize for future operations.

By the time that Black Basta was first identified in April 2022, many researchers already detected parallels with Conti; particularly, the similarities of both group's data leak sites and victim recovery portals. Conti opeartors denied the claim that they had rebranded as Black Basta, even going so far as to call the group "kids." However, leaked chats showing some Conti members questioning the targeting of the healthare sector, especially during the height of the COVID-19 pandemic, led to speculation that there might be a splintering within the group. For now, while is it impossible to state that Conti rebranded as or that some previous members of Conti are in Black Basta, the connections shared between both groups support the premise of some collaboration.

FIN7

Other researchers observed links to the Russian-speaking RaaS threat group, FIN7 (aka Carbanak/Cobalt Group/Carbon Spider). Active since 2013, the financially motivated group has been successful in their sophisticated and aggressive ransomware operations. A Mandiant report in 2022 detailed that FIN7 had links to other ransomware threat groups, notably Maze, Ryuk, Darkside, and BlackCat/ALPHV.

Demonstrating more hacktivist collaboration by June 2022, *Sentinel Labs* observed the first possible connection between FIN7 and Black Basta. Black Basta was observed utilizing an Endpoint Detection and Response (EDR) evasion tool, known to be used exclusively by its own members. A backdoor that FIN7 developed in 2018 and still uses was discovered within this EDR. This same backdoor connects to an IP address that FIN7 also uses reguarly. Furthermore, additional evidence of a connection between the groups is found in their attack techniques – specifically, the employment of Cobalt Strike. Like Conti, it is equally impossible to state that members of FIN7 are operators for or affiliates of Black Basta. However, the technical similiarties continue to show an indication that the two groups are closely related.

Other Ransomware Threat Groups

Black Basta has also exhibited similarities to the ransomware group known as BlackMatter. Specifically,

both groups implement a user verification on their Tor sites and share an interface resemblance on their respective leak sites. Agenda, another emerging ransomware group most likely tied to Russia, also shares parallels to Black Basta in its targeting the healthcare sector and with the same command for changing Windows passwords and rebooting in safe mode.

Mandiant reports that after U.S. sanctions on the Russian-speaking threat group, Evil Corp, in 2019, many loosely connected Russia-linked ransomware groups splintered into smaller cells and began to use different malware to obscure their identities and evade crackdowns. In June 2022, FBI Director Christopher Wray stated that U.S. officials are "running at full tilt against Russian cyber threats" by disrupting hacking groups and warning targets of imminent threats. However, threat groups like Conti, who pledged loyalty to the Kremlin during the inception of Russia's war in Ukraine, continue to demonstrate that task as more arduous, given the blurred lines between criminal ransomware and state-backed hacking efforts.

Defense and Mitigations

Black Basta's high-volume attacks in 2022 suggest that they will continue to attack and extort organizations. As RaaS threat groups become more prolific, healthcare organizatons should remain vigilant and strengthen their defenses against ransomware attacks. Organizations can take several multilayered actions to minimize their exposure to and the potential impact of a ransomware attack. While there is no specific set of recommendations to hinder Black Basta's custom capabilities, this Threat Profile presents a sample of mitigations, countermeasures, indicators of compromise, and other courses of action from various cybersecurity organizations and publications.

CISA Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

Check Point – How to Prevent a Ransomware Attack
https://blog.checkpoint.com/2022/10/20/check-point-research-analyzes-the-newly-emerged-black-basta-ransomware-alerts-organizations-to-adopt-prevention-best-practices/

KROLL – Black Basta Technical Analysis
https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis

QUADRANT – Technical Analysis: Black Basta Malware Overview
https://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview

Palo Alto Networks – Unit 42 – Threat Assessment: Black Basta Ransomware
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/#post-124665-_uht0xos2b4zh

Relevant HHS Reports

Conti Ransomware (Updated 09 March 2022)

Conti Ransomware and the Health Sector (08 July 2021)

Demystifying BlackMatter (02 September 2021)

HC3: Alert - Conti Ransomware Amplify Alert (30 September 2021)

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (09 May 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (01 March 2022)

HC3: Analyst Note - Cyber Threat Posed by BlackMatter RaaS Reduced to Guarded (Blue) (28 January 2022)

HC3: Analyst Note - Overview of Conti Ransomware (25 May 2021)

References

"Black Basta ransomware emerges." DXC Technology. Accessed 09 March 2023. https://dxc.com/us/en/insights/perspectives/report/dxc-security-threat-intelligence-report/june-2022/black-basta-ransomware-emerges

"Case Study: Technical Analysis: Black Basta Malware Overview." QUADRANT Information Security. 25 January 2023. https://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview

"Check Point Research analyzes the newly emerged Black Basta Ransomware, alerts organizations to adopt prevention best practices." Check Point. Accessed 09 March 2023. https://blog.checkpoint.com/2022/10/20/check-point-research-analyzes-the-newly-emerged-black-basta-ransomware-alerts-organizations-to-adopt-prevention-best-practices/

Cocomazzi, Antonio and Antonio Pirozzi. "Black Basta Ransomware – Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor." SentinelOne. 03 November 2022. https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

"Dark Web Profile: Black Basta Ransomware." SOCRadar Research. 16 December 2022. https://socradar.io/dark-web-profile-black-basta-ransomware/

Elsad, Amer. "Threat Assessment: Black Basta Ransomware." Palo Alto Networks – Unit 42. 25 August 2022. https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/#post-124665-_5ke50eq39xq0

Gonzalez, Ieriz Nicolle, et al. "Examining the Black Basta Ransomware's Infection Routine." Trend Micro Research. 09 May 2022. https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

Green, Stephen and Elio Biasiotto. "Black Basta – Technical Analysis." Kroll. 23 January 2023. https://www.kroll.com/en/insights/publications/cyber/black-basta-technical-analysis

"An In-Depth Look at Black Basta Ransomware." Avertium. 01 June 2022.

https://explore.avertium.com/resource/in-depth-look-at-black-basta-ransomware

"New Agenda Ransomware Targets Education and Healthcare Sectors." Cyware Social. 05 September 2022. https://cyware.com/news/new-agenda-ransomware-targets-education-and-healthcare-sectors-dd2592ee

"Ransomware Spotlight: Black Basta." Trend Micro Research. 01 September 2022. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

Toulas, Bill. "Black Basta ransomware gang linked to the FIN7 hacking group." Bleeping Computer. 03 November 2022. https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-linked-to-the-fin7-hacking-group/

Uberti, David. "Russia-Linked Ransomware Groups are Changing Tactics to Dodge Crackdowns." The Wall Street Journal. 02 June 2022. https://www.wsj.com/articles/russia-linked-ransomware-groups-are-changing-tactics-to-dodge-crackdowns-11654178400

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback