Mphasis
The Next Applied

Advisory: Black Basta Ransomware

Severity: Medium

Date: 13th May 2023

Overview

Black Basta ransomware emerged in April 2022 and went on a spree breaching over 90 organizations by Sept 2022. The rapidity and volume of attacks prove that the actors behind Black Basta are well-organized and well-resourced, and yet there has been no indications of Black Basta attempting to recruit affiliates or advertising as a RaaS on the usual darknet forums or crimeware marketplaces. This has led to much speculation about the origin, identity, and operation of the Black Basta ransomware group.

Technical Details

A Black Basta variants have been observed on Windows and Linux systems. Black Basta infections began with Qakbot delivered by email and macro-based MS Office documents, ISO+LNK droppers and .docx documents exploiting the MSDTC remote code execution vulnerability, CVE-2022-30190.

Manual reconnaissance is performed when Black Basta operators connect to victims through the Qakbot backdoor.

Reconnaissance utilities used by the operator are staged in a directory with deceptive names such as “Intel” or “Dell”, created in the root drive C:\.

For network scanning, Black Basta uses the SoftPerfect network scanner, netscan.exe. In addition, the WMI service is leveraged to enumerate installed security solutions. The ransomware will take steps to disable commonly used endpoint security products prior to initiating the encryption process.

Beyond the reconnaissance stage, Black Basta attempts local and domain level privilege escalation through a variety of exploits. We have seen the use of ZeroLogon (CVE-2020-1472), NoPac (CVE-2021-42287, CVE-2021-42278) and PrintNightmare (CVE-2021-34527).

Black Basta also employs an array of custom scripts and tools within their campaigns.

Black Basta's operational Techniques

- Black Basta's Initial Access Activity
- Enter the Black Basta Operator
- Black Basta Privilege Escalation Techniques
- Remote Admin Tools
- Black Basta Lateral Movement
- Impair Defenses
- Black Basta and the FIN7 Connection

How to Mitigate Black Basta Ransomware

A There are several steps that organizations can take to mitigate the risk of ransomware attacks:

1. **Educate employees:** Employees should be educated on the risks of ransomware and on how to identify and avoid phishing emails, malicious attachments, and other threats. They should be encouraged to report suspicious emails or attachments and avoid opening them or clicking on links or buttons.
2. **Enable multi-factor authentication:** Organizations should enable multi-factor authentication (MFA) for all user accounts to provide an additional layer of security. This can be done through the use of mobile apps, such as Google Authenticator or Microsoft Authenticator, or the use of physical tokens or smart cards.
3. **Audit and inventory:** Take an inventory of assets and data. Identify authorized and unauthorized devices and software. Audit event and incident logs
4. **Configure and monitor:** Manage hardware and software configurations. Grant admin privileges and access only when necessary to an employee's role. Monitor network ports, protocols, and services. Activate security configurations on network infrastructure devices such as firewalls and routers. Establish a software allowlist that only executes legitimate applications.
5. **Secure and defend:** Employ sandbox analysis to block malicious emails. Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network. Detect early signs of an attack such as the presence of suspicious tools in the system. Use advanced detection technologies such as those powered by AI and machine learning.
6. **Update and patch systems:** Organizations should regularly update and patch their systems to fix any known vulnerabilities and to prevent attackers from exploiting them. This includes updating the operating system, applications, and firmware on all devices and disabling any unnecessary or unused services or protocols.

Implement backup and disaster recovery: Organizations should implement regular backup and disaster recovery (BDR) processes, to ensure that they can recover from ransomware attacks or other disasters. This includes creating regular backups of all data and systems and storing these backups in a secure, offsite location. The backups should be tested regularly to ensure they work and can be restored quickly and easily.

Conclusion

The crimeware ecosystem is constantly expanding, changing, and evolving. FIN7 (or Carbanak) is often credited with innovating in the criminal space, taking attacks against banks and PoS systems to new heights beyond the schemes of their peers. As we clarify the hand behind the elusive Black Basta ransomware operation, we aren't surprised to see a familiar face behind this ambitious closed-door operation. While there are many new faces and diverse threats in the ransomware and double extortion space, we expect to see the existing professional criminal outfits putting their own spin on maximizing illicit profits in new ways.

IOCs

IP Addresses:

45[.]67[.]229[.]148

23[.]106[.]160[.]188

Hashes:

0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a

ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e

17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90

a54fef5fe2af58f5bd75c3af44f1fba22b721f34406c5963b19c5376ab278cd1

1d040540c3c2ed8f73e04c578e7fb96d0b47d858bbb67e9b39ec2f4674b04250

2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88

URL:

https[:]//aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd[.]onion

Reference Links

Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor - SentinelOne

Linux version of Black Basta ransomware encrypts VMware ESXi servers - Security Investigation (socinvestigation.com)

https://www.bleepingcomputer.com/search/?cx=partner-pub-0920899300397823%3A3529943228&cof=FORID%3A10&ie=UTF-8&q=black+basta