

BlackMatter Ransomware Explained: Delivery Methods, Tactics, and Targets

 cyberint.com/blog/dark-web/blackmatter-ransomware-explained-delivery-methods-tactics-and-targets

Adi Bleih

July 5, 2026

Dark Web

Introduction to BlackMatter Ransomware

Emerging in July 2021, BlackMatter is a ransomware-as-a-service (RaaS) platform that permits the developers of the ransomware to generate income through the actions of their cybercriminal associates, referred to as BlackMatter actors, who utilize it against targets. BlackMatter is potentially a reimagining of DarkSide, another RaaS that remained operational from September 2020 to May 2021. The individuals associated with BlackMatter have targeted numerous organizations based in the United States, demanding ransoms varying from \$80,000 to \$15,000,000, payable in cryptocurrencies such as Bitcoin and Monero.

Delivery Methods of BlackMatter Ransomware

The distribution of BlackMatter ransomware frequently occurs through phishing emails. Additionally, instances of employing Cobalt Strike and commercial-off-the-shelf (COTS) management and monitoring software have been noted. BlackMatter campaigns have also demonstrated associations with the exploitation of vulnerabilities in LDAP and SMB protocols.

In contrast to numerous cyberattacks that heavily rely on phishing as their entry point, BlackMatter seems to initiate its initial access primarily by targeting vulnerable edge devices and exploiting corporate credentials procured from alternate sources.

Although the possibility remains that in specific scenarios spear-phishing endeavors and the use of malevolent document payloads might lead to the deployment or retrieval of the compact ~80kb BlackMatter payload, such occurrences have not been observed in any investigations conducted by us.

Furthermore, apart from BlackMatter members capitalizing on weaknesses within infrastructural elements, such as remote desktop, virtualization, VPN appliances, or servers, operators involved in the initial access process associated with the group are likely to introduce their own tactics, techniques, and procedures (TTPs), possibly showing preferences for exploiting certain vulnerabilities over others.

The victim-specific ransom note advises the victim of both the data encryption and theft, advising them to install the TOR browser bundle so that the dark web negotiation site can be accessed.

The Impact of BlackMatter Ransomware

The BlackMatter ransomware sets its sights on a wide array of sectors, encompassing healthcare, telecommunications, banking, finance, education, government, and other essential infrastructure domains. Moreover, it has directed its attacks at a diverse range of entities, including hospitals, universities, major corporations, and small businesses.

About Check Point Exposure Management

Check Point Exposure Management is an intelligence-led, validation-driven, remediation-first unified platform that helps security teams move quickly and safely from exposure visibility to exposure reduction. Delivered through a single UI, it brings together threat intelligence, exposure prioritization, Agentic Exposure Validation, and safe remediation so teams can understand risk, prove exploitability, and act from one place.

[Schedule Your Demo Now](#)

BlackMatter Ransomware TTPS

Tactic Name	Technique
Impact	T1561 – Disk Wipe
Impact	T1486 – Data Encrypted for Impact
Exfiltration	T1567 – Exfiltration Over Web Service
Lateral Movement	T1021.002 – SMB/Windows Admin Shares
Discovery	T1007 – System Service Discovery
Discovery	T1057 – Process Discovery
Discovery	T1018 – Remote System Discovery
Credential Access	T1003.001 – LSASS Memory

Tactic Name	Technique
Persistence	T1133 – External Remote Services
Initial Access	T1133 – External Remote Services

BlackMatter Ransomware IOCs (Sample of 50)

Type	Date Added	Value
SHA-256	2026-06-10	f8850a32d2b21be78972966fa0cc0d809b997fa80eb27a2e0be95e83ffd21463
SHA-256	2026-06-10	bde1040f09977c860333464af390159fffeb3a2156f0cc0607369c3115c2f2da
SHA-256	2026-06-10	4044ad92b73412a3ca0984bd1f2c4895641c82c437418271893bef418398714e
SHA-256	2026-06-10	9e2d6e16e5572e6459bc257f4e6dc47b0b5f11663568bba2e9ad1e8a71165cd9
SHA-256	2026-06-10	ceed9b497256fd017f5073edd0bdcb9b1923b633ae5f9fdd95b46c634ebd747e
SHA-256	2026-06-10	29aa83fd9f601c6163c0c1b0cd6335c30e726e00337ac1312a7f42d2daffbefb
SHA-256	2026-06-10	370415c872a4ca6e1974cafb2950c3d31259ebdbba4952a81253272cd6b4f93b
SHA-256	2026-06-10	58e4c1a9530ea6236fffb02ad3fb9dff7c4462e71942a64f564373e7930cb8b4
SHA-256	2026-06-10	2d78ccb074929ea9134063306229d29fbd5416b8d2e720e4e91b92822ed49bbd
SHA-256	2026-06-10	7fc9ae64edb1864290156397d1baad0b56ce110623b73cd4d8c2b15ead3cdb07

Type	Date Added	Value
SHA-256	2026-06-10	7494ad77dfaef8c1d03c3025d442477b4a645f263bcf997114e66eb53422efa2
SHA-256	2026-06-10	7ac9fb3016067239ef2215fa65d2b82346a061fdb6f385e513f07c35936a4476
SHA-256	2026-06-10	1e3c621f7be6e0a8c220bdd01f7e242cd66fc666e0f91c43454d50bd06ae0359
SHA-256	2026-06-10	58e8419426fba3b971dd6eb448d6932a5b10247f3e1725e9e36469428abb138c
SHA-256	2026-06-10	8c047ba01ef0db2b2057190d6c35a7c0e6965f465b0015d17b8c59c3767b2cf1
SHA-256	2026-06-10	c527ebf0bb60a09e78bc1b4605573d93fccc7df0d3776120dffff79e4ffccf45
SHA-256	2026-06-10	43fbd94e73040bc4db717018ba42a6139a72e000e19314bcc51beed9699385f4
SHA-256	2026-06-10	fa361c712381c82552952e348c36dca949329db6ea6088c7228c3884ebb0bfe7
SHA-256	2026-06-10	e791ff4d28779b72bf7720b13bdb91a9be678c4b9f5a34e04d63d7a4b6f3777a
SHA-256	2026-06-10	0b525c358266f139dc9b8311f71dc0c93fe36939a8ed8aedcc3dbe510e82269d
URL	2026-06-02	http://178.16.54.109/lb25.exe
SHA-256	2026-06-01	1d9ba23a657f2c5eaea64c7a5aa96b628f0c23f371bfa6e74ac9bc9abc0efc93
SHA-256	2026-05-29	e040fac4e5b29fbe7606c2d39372935a8aee80a3167c7521efabc7c3e002a242

Type	Date Added	Value
SHA-256	2026-05-29	2e3876a4a2e1d7456dbc95a254b419de25a9b26d2bab3d98d8c9ff0faa43b48c
SHA-256	2026-05-29	80d36c0476b5de983271b65665bb6997eb58316bc3c151f04b045f45ef80784c
SHA-256	2026-05-29	1e399538c41be1c39566a00c95b78b39186510254e24562ec53a414ad74c23a1
SHA-256	2026-05-29	cf3befb087ca768d1dcd4eee9dc75c9adb1ca26bce74865c9005da1c2c794274
SHA-256	2026-05-29	d715b248f71cd6ba4fcc78b89e9184ff5f0a04b9d02790bcb30e13c040d3973
SHA-256	2026-05-29	bc93fb67cf4dba8c35e91b551ca3190db25ffa4a36f821bc5a6b900927470fb9
SHA-256	2026-05-29	f016df16d0f34aaae36bf10e0ca6bccdce2a4d552fcc6444e6f48318ef0b2c4a
SHA-256	2026-05-29	a397bea4c70bf3264348c88fca652fcb2d421832672fa58a790af67bf419469
SHA-256	2026-05-29	93da3f615d041dc37a4b3db4a3d0c60bfd3c3fb1fc3ff4d5b764c646b629da7b
SHA-256	2026-05-29	0cd5240c696194cf2eb701cd4d4ca81e7f17612a4042ebb56959008d66537b4b
SHA-256	2026-05-29	92fc7f45d4968df95bc082220680c9ebd6a381a9467f77493878af031454d633
SHA-256	2026-05-29	c9417d4683324c34c7b976395c01f79150a626966e27144244214423aa64ccde
SHA-256	2026-05-29	1985db0655bca27343a13d8607904c53a292459083daa8c92ae2f71a5408b40a

Type	Date Added	Value
SHA-256	2026-05-29	53e315669d72051a4add2e28938733dc116bb46fdc05dcda1958e7ea466812ed
SHA-256	2026-05-29	8796e69f738fceb99fd177a5536dbccf5112ffa202a8b05be10ab45e600e289b
SHA-256	2026-05-29	326536a0bcb9198049da10f4873446393c0f7ceb91098aecdd39a94f6d691112
SHA-256	2026-05-29	06fe6a157bd3f67ae9f7cdf3478a0db670c2772b584cae5900d2473b6b109bb7
SHA-256	2026-05-29	34f9b16d363f1bd44d912a62ee0745985ac696b6c4aaf4799a9b2b37d11720e8
SHA-256	2026-05-26	9d8526b0ecc2081eab5ec68b7063ffe8dbd987681b77b2e8d96a0c8979b1f8a
SHA-256	2026-05-26	dc870a75269409d7ccee7984b7c2b6b03f29aabea10a314bf1a068aba23452e4
SHA-256	2026-05-26	34ca794e716157290147b180a0d65d47ddf6dedde646957324d40bf299289294
SHA-256	2026-05-26	cdc7d79ae4215dccf60882afb6c3abee6b95d9db7c1587746fc8d533d1631e9d
URL	2026-03-18	http://158.94.211.162/3.exe
URL	2026-03-18	http://158.94.211.162/2.exe
URL	2026-03-18	http://158.94.211.162/1.exe
URL	2026-03-18	http://158.94.211.162/10.exe

Type	Date Added	Value
URL	2026-03-18	http://158.94.211.162/7.exe