SystemBC (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:06:27 UTC

SystemBC is a multiplatform proxy malware active since August 2019. It creates SOCKS5 network tunnels in the victim's network and connects to its C2 server using a custom, RC4-encrypted protocol. It can also download and execute additional malware, with payloads either written to disk or mapped into memory. The SystemBC kit, including the C2 panel, server, and malware executables, is sold in underground forums.

2025-09-18 · Lumen ·
SystemBC – Bringing the Noise
SystemBC SystemBC 2025-07-18 · Arctic Wolf · Arctic Wolf Labs Team
Greedy Sponge Targets Mexico with AllaKore RAT and SystemBC
AllaKore SystemBC 2025-04-24 · Mandiant · Mandiant
M-Trends 2025 Report
Akira Black Basta LockBit SystemBC GootLoader LockBit WIREFIRE Akira Black Basta Cobalt Strike LockBit
RansomHub SystemBC Pink Sandstorm 2025-01-27 · The DFIR Report · MittenSec, MyDFIR, r3nzsec
Cobalt Strike and a Pair of SOCKS Lead to LockBit Ransomware
GhostSocks LockBit SystemBC 2024-12-04 · Rapid7 · Tyler McGraw
Black Basta Ransomware Campaign Drops Zbot, DarkGate, and Custom Malware
Black Basta Cobalt Strike DarkGate SystemBC Zloader 2024-08-26 · The DFIR Report · The DFIR Report
BlackSuit Ransomware
BlackSuit Cobalt Strike SystemBC 2024-08-12 · Rapid7 · Tyler McGraw
Ongoing Social Engineering Campaign Refreshes Payloads
Black Basta Cobalt Strike GhostSocks Lumma Stealer SystemBC 2024-07-29 · Mandiant · Ashley Pearson, Jake Nicastro, Joseph Pisano, Josh Murchie, Joshua Shilko, Raymond Leong
UNC4393 Goes Gently into the SILENTNIGHT
Black Basta QakBot sRDI SystemBC Zloader UNC3973 UNC4393 2024-05-30 · Europol · Europol
Largest ever operation against botnets hits dropper malware ecosystem
BumbleBee IcedID SmokeLoader SystemBC TrickBot 2024-05-15 · Microsoft · Microsoft Threat Intelligence
Threat actors misusing Quick Assist in social engineering attacks leading to ransomware
Black Basta Cobalt Strike QakBot SystemBC 2024-01-19 · Kroll · David Truman
Inside the SYSTEMBC Command-and-Control Server
SystemBC 2023-11-12 · Github (vc0RExor) · Aaron Jornet
The Swiss Knife: SystemBC | Coroxy
SystemBC 2023-10-12 · YouTube (FIRST) · Aditya K. Sood
"Compromising the Keys to the Kingdom" - Exfiltrating Data to Own and Operate the Exploited Systems
Loki RAT SystemBC 2023-09-12 · FIRSTCON · Aditya K. Sood
Compromising the Keys to the Kingdom: Exfiltrating Data to Own and Operate the Exploited Systems (Slides)
Loki RAT SystemBC 2023-09-12 · · ANSSI · ANSSI

FIN12: A Cybercriminal Group with Multiple Ransomware

BlackCat Cobalt Strike Conti Hive MimiKatz Nokoyawa Ransomware PLAY Royal Ransom Ryuk SystemBC

2023-08-23 · Logpoint · Anish Bogati, Nischal khadgi

Defending Against 8base: Uncovering Their Arsenal and Crafting Responses

8Base Phobos SmokeLoader SystemBC 2023-08-10 · Kaspersky · Kurt Baumgartner

Focus on DroxiDat/SystemBC

SystemBC 2023-06-28 · vmware · Bria Beathley, Dana Behling, Deborah Snyder, Fae Carlisle

8Base Ransomware: A Heavy Hitting Player

8Base Phobos SmokeLoader SystemBC 2023-06-27 · SecurityIntelligence · Charlotte Hammond, Ole Villadsen

The Trickbot/Conti Crypters: Where Are They Now?

Black Basta Conti Mount Locker PhotoLoader Royal Ransom SystemBC TrickBot 2023-06-22 · Reliaquest · Caroline Fenstermacher

Goot to Loot - How a Gootloader Infection Led to Credential Access

GootLoader SystemBC 2023-05-15 · CrowdStrike · CrowdStrike

Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks

BlackCat SystemBC 2023-04-19 · Symantec · Threat Hunter Team

Play Ransomware Group Using New Custom Data-Gathering Tools

PLAY SystemBC 2023-04-18 · Mandiant · Mandiant

M-Trends 2023

QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate 2023-03-30 · eSentire · eSentire Threat Response Unit (TRU)

eSentire Threat Intelligence Malware Analysis: BatLoader

BATLOADER Cobalt Strike ISFB SystemBC Vidar 2023-02-14 · Cybereason · Cybereason Incident Response (IR) team

GootLoader - SEO Poisoning and Large Payloads Leading to Compromise

GootLoader Cobalt Strike SystemBC 2023-02-09 · cyber.wtf blog · Hendrik Eckardt

Defeating VMProtect’s Latest Tricks

SystemBC 2023-01-23 · Kroll · Elio Biasiotto, Stephen Green

Black Basta – Technical Analysis

Black Basta Cobalt Strike MimiKatz QakBot SystemBC 2023-01-16 · Intrinsec · Intrinsec

ProxyNotShell – OWASSRF – Merry Xchange

Cobalt Strike SystemBC 2022-10-28 · velociraptor · Matt Green

Windows.Carving.SystemBC - SystemBC RAT configuration Purser for Velociraptor

SystemBC 2022-10-10 · RiskIQ · Microsoft Threat Intelligence Center (MSTIC)

DEV-0832 Leverages Commodity Tools in Opportunistic Ransomware Campaigns

BlackCat Mount Locker SystemBC Zeppelin 2022-09-21 · BitSight · João Batista

SystemBC: The Multipurpose Proxy Bot Still Breathes

SystemBC 2022-09-06 · CISA · CISA, FBI, MS-ISAC, US-CERT

Alert (AA22-249A) #StopRansomware: Vice Society

Cobalt Strike Empire Downloader FiveHands HelloKitty SystemBC Zeppelin 2022-08-30 · Cisco · Vanja Svajcer

ModernLoader delivers multiple stealers, cryptominers and RATs

Coinminer DCRat ModernLoader RedLine Stealer SapphireMiner SystemBC 2022-06-01 · Elastic · Andrew Pease,

Daniel Stepanic, Derek Ditch, Salim Bitam, Seth Goodwin

CUBA Ransomware Campaign Analysis

Cobalt Strike Cuba Meterpreter MimiKatz SystemBC 2022-05-24 · BitSight · BitSight, João Batista, Pedro Umbelino

Emotet Botnet Rises Again

Cobalt Strike Emotet QakBot SystemBC 2022-05-09 · Microsoft Security · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center

Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself

Griffon BazarBackdoor BlackCat BlackMatter Blister Gozi LockBit Pandora Rook SystemBC TrickBot 2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself

AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT 2022-04-12 · AhnLab · ASEC Analysis Team

SystemBC Being Used by Various Attackers

Emotet SmokeLoader SystemBC 2022-03-04 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

SystemBC, PowerShell version

SystemBC 2022-01-19 · Mandiant · Adrian Sanchez Hernandez, Ervin James Ocampo, Paul Tarter

One Source to Rule Them All: Chasing AVADDON Ransomware

BlackMatter Avaddon BlackMatter MedusaLocker SystemBC ThunderX 2021-06-07 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Inside the SystemBC Malware-As-A-Service

Ryuk SystemBC TrickBot 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 2021-05-10 · F-Secure · Callum Roxan, Sami Ruohonen

Prelude to Ransomware: SystemBC

SystemBC 2021-04-21 · SophosLabs Uncut · Anand Aijan, Andrew Brandt, Markel Picado, Michael Wood, Sean Gallagher, Sivagnanam Gn, Suriya Natarajan

Nearly half of malware now use TLS to conceal communications

Agent Tesla Cobalt Strike Dridex SystemBC 2021-04-01 · Reversing Labs · Robert Simmons

Code Reuse Across Packers and DLL Loaders

IcedID SystemBC 2021-02-25 · FireEye · Brendan McKeague, Bryce Abdo, Van Ta

So Unchill: Melting UNC2198 ICEDID to Ransomware Operations

MOUSEISLAND Cobalt Strike Egregor IcedID Maze SystemBC 2021-02-03 · InfoSec Handlers Diary Blog · Brad Duncan

Excel spreadsheets push SystemBC malware

Cobalt Strike SystemBC 2020-12-16 · SophosLabs Uncut · Sean Gallagher, Sivagnanam Gn

Ransomware operators use SystemBC RAT as off-the-shelf Tor backdoor

SystemBC 2020-10-14 · Sophos · Sean Gallagher

They’re back: inside a new Ryuk ransomware attack

Cobalt Strike Ryuk SystemBC 2019-07-31 · Proofpoint · Dennis Schwarz, Kade Harmon, Kafeine, Proofpoint Threat Insight Team

SystemBC is like Christmas in July for SOCKS5 Malware and Exploit Kits

SystemBC

▶ [TLP:WHITE] win_systembc_auto (20251219 | Detects win.systembc.)
