




# SystemBC Malware's C2 Server Analysis Exposes Payload Delivery Tricks

 Jan 25, 2024

 Ravie Lakshmanan

Remote Access Trojan



Cybersecurity researchers have shed light on the command-and-control (C2) server workings of a known malware family called **SystemBC**.

"SystemBC can be purchased on underground marketplaces and is supplied in an archive containing the implant, a command-and-control (C2) server, and a web administration portal written in PHP," Kroll [said](#) in an analysis published last week.

The risk and financial advisory solutions provider said it has witnessed an increase in the use of malware throughout Q2 and Q3 2023.

SystemBC, [first observed](#) in the wild in 2018, allows threat actors to remote control a compromised host and deliver additional payloads, including trojans, Cobalt Strike, and ransomware. It also features support for launching ancillary modules on the fly to expand on its core functionality.

Top 2024 SaaS Security Risks

READ THE REPORT



A standout aspect of the malware revolves around its use of SOCKS5 proxies to mask network traffic to and from C2 infrastructure, acting as a persistent access mechanism for post-exploitation.

Customers who end up purchasing SystemBC are provided with an installation package that includes the implant executable, Windows and Linux binaries for the C2 server, and a



XM Cyber on Operationalizing the Continuous Threat Exposure Management (CTEM) Framework by Gartner

Download Now





See your top 5 SaaS security risks.

Misconfigurations, data exfiltration, data destruction, & more.



## Trending News

- ...

New Grandoreiro Banking Malware Variants Emerge with Advanced Tactics to Evade Detection
- ...

Eliminating AI Deepfake Threats: Is Your Identity Security AI-Proof?
- ...

Notorious Hacker Group TeamTNT Launches New Cloud Attacks for Crypto Mining
- ...

Permiso State of Identity Security 2024: A Shake-up in Identity Security Is Looming Large
- ...

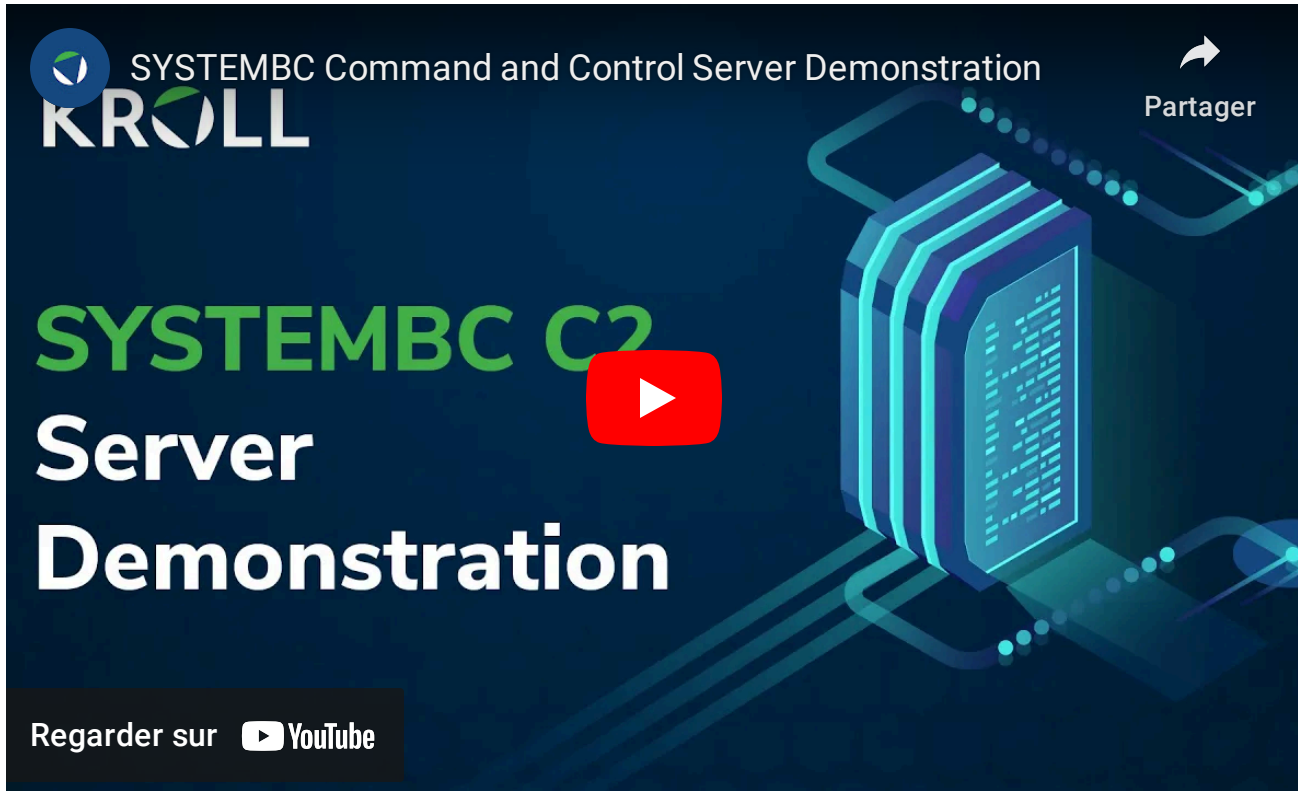
Researchers Uncover OS Downgrade Vulnerability Targeting Microsoft Windows Kernel

PHP file for rendering the C2 panel interface, alongside instructions in English and Russian that detail the steps and commands to run.

The C2 server executables – "server.exe" for Windows and "server.out" for Linux – are designed to open up no less than three TCP ports for facilitating C2 traffic, inter-process communication (IPC) between itself and the PHP-based panel interface (typically port 4000), and one for each active implant (aka bot).

The server component also makes use of three other files to record information regarding the interaction of the implant as a proxy and a loader, as well as details pertaining to the victims.

The PHP-based panel, on the other hand, is minimalist in nature and displays a list of active implants at any given point of time. Furthermore, it acts as a conduit to run shellcode and arbitrary files on a victim machine.



"The shellcode functionality is not only limited to a reverse shell, but also has full remote capabilities that can be injected into the implant at runtime, while being less obvious than spawning cmd.exe for a reverse shell," Kroll researchers said.

The development comes as the company also shared an analysis of an updated version of [DarkGate](#) (version 5.2.3), a remote access trojan (RAT) that enables attackers to fully compromise victim systems, siphon sensitive data, and distribute more malware.

"The version of DarkGate that was analyzed shuffles the Base64 alphabet in use at the initialization of the program," security researcher Sean Straw [said](#). "DarkGate swaps the last character with a random character before it, moving from back to front in the alphabet."

Kroll said it identified a weakness in this custom Base64 alphabet that makes it trivial to decode the on-disk configuration and keylogging outputs, which are encoded using the alphabet and stored within an exfiltration folder on the system.

"This analysis enables forensic analysts to decode the configuration and keylogger files without needing to first determine the hardware ID," Straw said. "The keylogger output files contain keystrokes stolen by DarkGate, which can include typed passwords, composed emails and other sensitive information."

... [New LightSpy Spyware Version Targets iPhones with Increased Surveillance Tactics](#)

... [Researchers Uncover Vulnerabilities in Open-Source AI and ML Models](#)

... [A Sherlock Holmes Approach to Cybersecurity: Eliminate the Impossible with Exposure...](#)

... [Chinese Hackers Use CloudScout Toolset to Steal Session Cookies from Cloud Services](#)

... [CERT-UA Identifies Malicious RDP Files in Latest Attack on Ukrainian Entities](#)

... [U.S. Government Issues New TLP Guidance for Cross-Sector Threat Intelligence Sharing](#)


— Popular Resources

... [Get the 24-Page Guide Every CISO Needs: AI-Driven NDR and Cyber Resilience](#)

... [Check Out This Demo on How to Identify and Patch SaaS Vulnerabilities Before Hackers Do](#)

... [Free Tool Uncovers Weak Passwords and Policies in Your Active Directory](#)

... [Is Your Security Operations Center \(SOC\) Underperforming? Here's How to Fix It Fast](#)

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.

 [Tweet](#)

 [Share](#)

 [Share](#)

 [Share](#)

## CYBERSECURITY WEBINARS

[Secure Your Certificates, Fast!](#)

### Learn to Automate Certificate Replacement to Avoid Disruptions

Prevent disruptions from certificate revocations with fast, automated solutions for continuity.

[Claim Your Spot](#)

[Make Cybersecurity Memorable!](#)

### Learn How to Turn Boring Security Training into Stories They'll Love

Discover how Huntress SAT transforms security training with storytelling, gamification, and real-world examples

[Join the Session](#)

### — Breaking News

### — Cybersecurity Resources



#### Ultimate Guide to Cloud Security

Tackle the unique challenges of cloud security with this expert guide.



#### Permiso Security's 2024 State of Identity Security Report

More than 90% of respondents expressed concern over their team and tooling's ability to detect identity-based attacks. Learn about critical gaps in security programs and what environments pose the most risk to security teams. Download the Report.



#### CISO, Enhance Your Cyber Risk Reporting to the Board

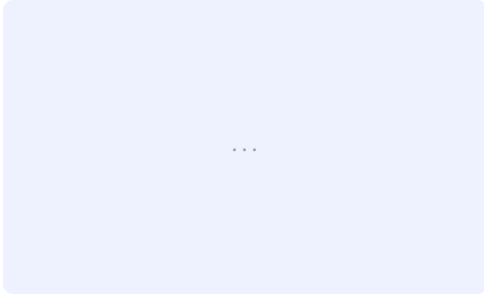
Struggling to convey cybersecurity risks to your board? Our eBook offers actionable insights for CISOs, helping you present accurate, meaningful reports with confidence. Elevate your board presentations—download your guide today.




#### 2024 GigaOm Report: Top SSPM Solutions for Protecting SaaS Environments

Explore GigaOm's 2024 SSPM Radar Report with top vendor insights for securing SaaS data.


### — Expert Insights / [Videos](#) [Articles](#)




#### Master Privileged Access Management: Best Practices to Implement

 October 14, 2024


[Read](#) →




#### Will the Small IoT Device OEM Survive?

 October 07, 2024


[Read](#) →




#### Security Operations for Non-Human Identities

 September 28, 2024

[Watch](#) →



#### The Microsoft 365 Backup Game Just Changed: Ransomware Recovery Revolutionized

 September 19, 2024

[Read](#) →

Get Latest News in Your Inbox

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders – all for free.

Your e-mail address

>

Connect with us!



925,500 Followers



601,000 Followers



22,700 Subscribers



147,000 Followers



1,890,500 Followers



132,000 Subscribers

Company

- About THN
- Advertise with us
- Contact

Pages

- Webinars
- Deals Store
- Privacy Policy

Deals

- Hacking
- Development
- Android

 RSS Feeds

 Contact Us