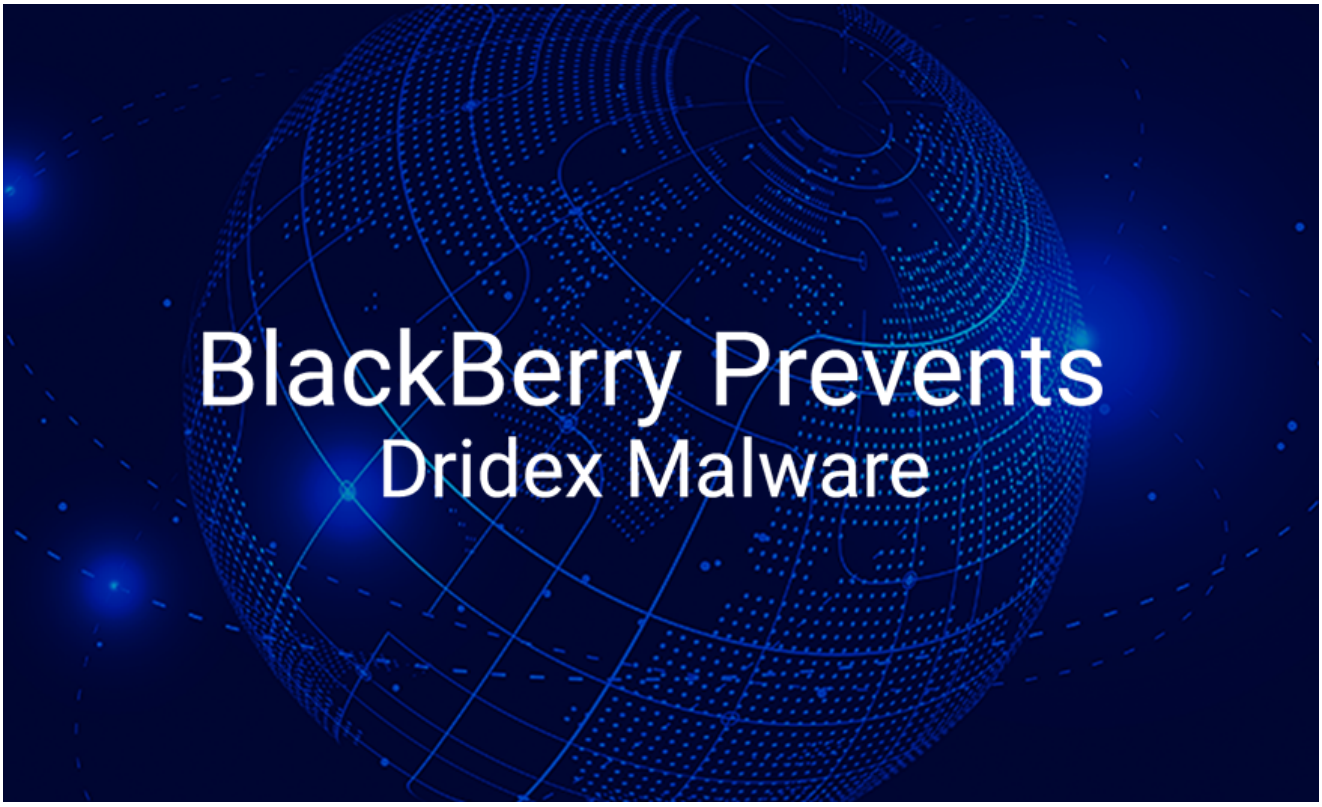
BlackBerry Prevents: Threat Actor Group TA575 and Dridex Malware

blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware

The BlackBerry Research & Intelligence Team



The BlackBerry Research & Intelligence team has been tracking and monitoring Cobalt Strike team servers associated with the threat actor TA575, a financially motivated cybercrime group and prolific Dridex affiliate. They are well-known for conducting mass spam campaigns that use malicious document lures to deliver malware such as Dridex, Qakbot, and WastedLocker.

Since February 2021, TA575 has deployed more than 50 Cobalt Strike team servers. These servers use unique values in their configurations that have allowed BlackBerry researchers to identify disparate infrastructure that had previously been flying under the radar.

Portions of this infrastructure have been used by thousands of Cobalt Strike “Beacons” and malicious document stagers across several distinct malspam campaigns. In more recent offensives, such as the Fake Kaseya VSA phishing campaign first reported by Trustwave in early July, the team server infrastructure was used for staging further Dridex payloads.

BlackBerry Cyber Suite and BlackBerry Guard stop these attacks.

BlackBerry customers can feel confident that our AI-driven BlackBerry® Cyber Suite, as well as our Managed Detection & Response (MDR) solution BlackBerry® Guard, are well-equipped to mitigate the risks posed by threat actors such as TA575:

- BlackBerry® Protect provides automated malware prevention, application and script control, memory protection, and device policy enforcement.
- BlackBerry® Optics extends the threat prevention by using artificial intelligence (AI) to prevent security incidents. It provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.
- The BlackBerry Mobile Threat Defense (MTD) solution prevents and detects advanced malicious threats at the device and application levels. It combines the mobile endpoint management capabilities of BlackBerry® Unified Endpoint Manager (UEM) with advanced AI-driven threat protection, to get in front of malicious cyberattacks in a Zero Trust environment.
- BlackBerry® Persona creates trust based on behavior analytics, app usage, and network and process invocation patterns. It uses adaptive risk scoring to provide continuous authentication.
- BlackBerry Guard customers are proactively protected from Dridex malware attacks. Our 24/7 MDR solution customers receive:
    - Alerts monitored in real-time
    - Corrective policies applied while discovering gaps in policy implementation
    - Prioritized threat hunting
    - The latest threat intelligence for fast-moving threats

Prevention First

At BlackBerry, we take a prevention-first and AI-driven approach to cybersecurity. Putting prevention first neutralizes malware before the exploitation stage of the kill-chain.

By stopping malware at this stage, BlackBerry® solutions help organizations increase their resilience. It also helps reduce infrastructure complexity and streamline security management to ensure your business, people, and endpoints are secure.

BlackBerry Assistance

The BlackBerry Incident Response team can work with organizations of any size and across any vertical, to evaluate and enhance their endpoint security posture and proactively maintain the security, integrity, and resilience of their network infrastructure.

For emergency assistance, please email us at DLIR@blackberry.com, or use our handraiser form.

Learn more about the latest cybersecurity threats and threat actors in the BlackBerry 2021 Annual Threat Report.

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.