prdeadlines

Radware alert: Fancy Lazarus DDoS extortion group is back with new campaign focused on unprotected assets across all industries

Radware onboards numerous customers with Fancy Lazarus ransom letters in recent weeks

SYDNEY, June 15, 2021—Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, published a cybersecurity alert warning that Fancy Lazarus, a well-known distributed denial of service (DDoS) extortionist, has resurfaced with a new campaign focused on organisations with unprotected assets across all sizes of companies in all industries.

Less than a year ago, a Ransom DDoS threat actor posing as 'Fancy Bear' and 'Lazarus Group' was targeting specific industries such as finance, travel and e-commerce organisations and was blind to whether these organisations had DDoS protection or not. This earlier campaign turned out to be one of the most extensive and longest-running DDoS extortion campaigns in history.

Lately, Radware has identified an increase in emergency onboardings from new customers that have had DDoS ransomware threats. In recent weeks, Radware has been monitoring an increase of activity from a threat actor calling himself Fancy Lazarus targeting organisations with assets that were supposedly not adequately protected and inviting them to pay a ransom rather than endure devastating DDoS attacks.

In their letters, the extortionists give their victims seven days to buy the Bitcoin and pay the ransom before they start their DDoS attacks. Each day after the deadline passes without payment increases that fee. The ransom demand varies between targets and seems to be adjusted to a target's reputation and size.

The ransom demand is also less expansive compared to the huge demands of 10 and 20 bitcoin (currently, about $370,000 and $740,000 at time of writing) witnessed from last summer's campaigns. Demands now generally vary between 0.5 Bitcoins ($18,500) and five Bitcoins ($185,000) and increase by the same amounts for every day the deadline is missed.

"This is the first time we are seeing the bad actors selectively target organisations and favour those with unprotected assets for their ransom letters," said Pascal Geenens, Director of Threat Intelligence, Radware. "This implies that malicious actors are leveraging Border Gateway Protocol routing information to detect whether targets are protected by always-on cloud protection services.

In addition, we're seeing that ransom DDoS, which traditionally was an event limited in time with yearly spikes, is now becoming a persistent threat, and should be considered an integral part of the DDoS threat landscape."

Reports from victims impacted by follow-through attacks of this extortion campaign confirm this observation. Most Internet Service Providers (ISP) and Cloud Service Provider (CSP) victims were equipped with DDoS mitigation services to protect their customers. However, it appears that not all of them were prepared for large, globally distributed attacks targeting their DNS servers or saturating their internet links.

Very large and globally distributed DDoS attacks can be effectively mitigated only by stopping malicious traffic closest to its source and never allowing multiple geographically distributed traffic streams to flock. Only globally distributed and anycasted protection services are effective against these kinds of DDoS attacks.

Geenens added: "The recent uptick in criminal activity should be a strong reminder to enterprises, ISPs and CSPs of any size and industry to assess the protection of their essential services and internet connections and plan against globally distributed DDoS attacks aimed at saturating links.

This is especially in the case of service providers and their DNS services. We believe hybrid DDoS solutions provide the best of both worlds with on-premises protection against all types of DDoS attacks while automatically diverting to a cloud DDoS Service when the attack risks saturating the internet link."

About Radware

Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection and availability services to enterprises globally. Radware's solutions empower enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, and Radware Mobile for iOS and Android,.

Media contact :
Radware
Joel Arabia
joel.arabia@radware.com

Contacts

David Frost
(02) 7903 9567
mailto: david.frost@prdeadlines.com