prdeadlines

Radware cyber security alert - Global ransom DDoS campaign targeting finance, travel and e-commerce

Radware is following a global ransom DDoS campaign targeting organisations in the finance, travel and e-commerce verticals. Additionally multiple internet service providers have been reporting DDoS attacks targeting their DNS infrastructure.

Global ransom DDoS campaigns

Since mid- August, Radware has been tracking several extortion requests from threat actors posing as 'Fancy Bear', 'Armada Collective', and 'Lazarus Group.'

Letters are being delivered via email and typically contain victim-specific data such as Autonomous System Numbers (ASN) or IP addresses of servers or services they will target if their demands are not fulfilled. It is a global campaign with threats reported from organisations in finance, travel and e-commerce in APAC, EMEA and North America.

The ransom fee is initially set at 10 BTC, which is equivalent to $113,000 at the time of the extortion. Some fees are set as high as 20 BTC (approximately $226,000). These demands are larger versus 2019 campaigns that typically requested between 1 BTC or 2 BTC.

Ransom letters threaten cyber attacks of over 2Tbps if payment is not made. To prove the letter is not a hoax, authors indicate when they will launch a demonstration attack.

The letter indicates that if payment is not made prior to the deadline, the attack will continue and the fee will increase by 10 BTC (approximately $113,000) for each missed deadline. Each letter contains a Bitcoin wallet address for payment. The wallet address is unique for each target and allows the actor to track payments.

The ransom letters are very similar in their terms and demands. Threats and advertised capabilities follow the same indicators from earlier reports.

Follow up and follow through

Radware has evidence of malicious actors following up on their initial demand. In follow up messages, threat actors underscore that the unique Bitcoin address from the initial letter is still empty and reiterate the seriousness of the threat. They also provide keywords and organisation names so the target organisation can search for recent DDoS disruptions, followed by the rhetorical question "You don't want to be like them, do you?"

The threat actors state they prefer payment over attack and allow the target to reconsider paying. The threat actor will often extend the deadline by one day.

In many cases the ransom threat Is followed by cyber attacks ranging from 50Gbps to 200Gbps. The attack vectors include UDP and UDP-Frag floods, some leveraging WS-Discovery amplification, combined with TCP SYN, TCP out-of-state, and ICMP Floods.

Radware advises

Ransom letters with comparable indicators should be taken seriously. The letters are often followed by DDoS attacks. These attacks are not at a level of complexity/amplitude that prevent mitigation if the right protection is in place. Radware has seen faster and better mitigation by leveraging hybrid always-on protection compared to asymmetric routed cloud protections.

Radware advises against paying the ransom demand as there is no guarantee the malicious actors will honour the terms and it 'identifies' the target organisation as one that is willing to pay under threat. Paying the ransom funds the malicious operation and allows the bad actors to improve their capabilities and motivates them to continue their campaign.

Internet service provider attacks

Since the last week of August, Radware has been tracking several internet service providers (ISPs) in Europe that have reported disturbances caused by DDoS attacks. The attacks are primarily targeting the DNS infrastructure of the providers and disrupt customers that use the provider's DNS servers to resolve internet hostnames. Several providers were impacted and some have suffered multiday disturbances across their customer base.

Currently, Radware has no immediate link between the ISP attacks and the ransom campaign. There are some ransom letters that indicate that the demonstration attack will target DNS infrastructure, but that is the extent of similarities. There have been no reports of ransom letters to ISP targets, only from finance, travel and e-commerce.

Effective DDoS protection essentials

Hybrid DDoS Protection - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation.

Behavioural-based detection - quickly and accurately identify and block anomalies while allowing legitimate traffic through.

Real-time signature creation - promptly protect from unknown threats and zero-day attacks

A cyber security emergency response plan - a dedicated emergency team of experts who have experience with Internet of Things security and

handling IoT outbreaks

Intelligence on Active Threat Actors – high fidelity, correlated and analysed date for pre-emptive protection against currently active known attackers

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective web application security essentials

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate – using negative and positive security models for maximum accuracy

Auto policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premise, out-of-path, virtual or cloud-based

Learn more at DDoS warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au