



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Extortion: Profit-Motivated Cyber Tactics On the Rise

November 25, 2015

TLP: WHITE | *The NJCCIC assesses with high confidence that profit-motivated cyber extortion schemes such as ransomware and ransom-demanding distributed denial of service (DDoS) threats are likely to persist as effective and lucrative criminal tactics into 2016, with cumulative US losses likely to continue climbing into the hundreds of millions of dollars.* These schemes have steadily grown in frequency and sophistication over the last year, with numerous new variants and capabilities emerging, such as the [fourth iteration](#) of the damaging CryptoWall ransomware family and a new ransomware [strain targeting Linux-based](#) operating systems often found on web servers. In addition to file-encrypting malware, other tactics are being employed to extort victims, such as blackmail and threats of disruptive DDoS attacks.

- A cyber threat actor known as DD4BC—short for “DDoS for Bitcoin”—gained [international attention](#) throughout 2015 for a ransom-demanding [DDoS campaign](#) impacting financial institutions, media and entertainment companies, online gaming, and retailers. DD4BC was attributed to DDoS attacks that targeted [four Atlantic City casinos](#) in July. Victims of these tactics typically receive an email warning of an impending attack on their network and demanding ransom payment in order to prevent the attack. Shortly thereafter, the actor conducts a brief DDoS attack on the target to demonstrate their capabilities, followed by additional threats of larger, sustained attacks.
- In early October, the technology and security firm Cisco [announced](#) the disruption of a criminal network utilizing the Angler [exploit kit \(EK\)](#) to distribute ransomware and target up to 90,000 victims per day. Researchers estimated that the primary threat actor generated as much as \$30 million annually through ransomware campaigns.
- In late October, the Cyber Threat Alliance (CTA) released an investigative [report](#) on the most prevalent [ransomware](#) variant, CryptoWall 3. Since appearing in January 2015, over 400,000 attempted CryptoWall 3 infections were observed, mostly targeting North American systems, and CTA estimated \$325 million in damages to victims. Two-thirds of infections were achieved through phishing emails containing attachments with filenames such as “invoice” or “statement”, and remaining infections occurred through [EKs](#), most often the Angler EK.
- In June, the [FBI identified](#) Cryptowall as the most significant ransomware threat targeting US businesses and individuals. Between April 2014 and June 2015, the FBI received 992 CryptoWall-related complaints with victims reporting losses totaling over \$18 million. These losses go beyond the demanded ransom, ranging from \$200 to \$10,000, as victims incur additional costs such as network mitigation, data or productivity loss, or legal expenses.

Ransomware Mitigation

First and foremost, the NJCCIC recommends against paying ransom of any kind, as this only perpetuates these crimes and encourages other criminals to pursue these tactics. Moreover, paying the ransom does not guarantee decryption of data or prevention of attacks. The most effective preventative measure to avoid ransomware infections is to ensure all users are trained in best practices to recognize phishing emails and to never click on links or download attachments in unsolicited emails. Additionally, users should be trained on safe web browsing practices to avoid drive-by downloads and [malicious advertising](#). Ensure antivirus software is set to automatically update and run scans regularly. Lastly, all operating systems, software, web browsers, and plugins should be updated as soon as patches are made available.

DDoS Mitigation

The NJCCIC recommends organizations establish DDoS mitigation protection with their Internet Service Providers or other third-party vendors, increasing the likelihood of identifying and deflecting malicious traffic. Additionally, organizations should implement the recommended mitigation strategies outlined in the Center for Internet Security’s comprehensive [Guide to DDoS Attacks](#). If a DDoS ransom threat is received, we urge our members to not pay the ransom, and instead engage with third-party mitigation services or report the incident to the [NJCCIC](#).

Traffic Light Protocol: **WHITE** information may be distributed without restriction.