rewterz

2022

THREAT INTEL INSIGHTS

AUGUST 2022

1

SEMICONDUCTOR COMPONENT MANUFACTURER SEMIKRON HIT BY A RANSOMWARE ATTACK

Semikron, an independent producer of power semiconductor components with headquarters in Germany, becomes the victim of a ransomware cyberattack. Semikron claims to be one of the world’s leading power engineering component manufacturers. Its technologies power 35% of wind turbines installed yearly.

2

STORMFIBER WEBSITE DEFACEMENT

StormFiber, a Pakistani internet service provider (ISP) website, was recently hacked by India based hacktivist. The company attributed the breach to a “WordPress vulnerability.”Web defacement is an attack in which malicious parties infiltrate a web page and replace its content with their own messages.

3

TAIWAN GOVERNMENT WEBSITES HIT WITH DDOS ATTACK

During US House Speaker Nancy Pelosi’s visit to Taiwan, major Taiwan government websites were temporarily forced offline by a distributed denial of service (DDoS) attack. Government English portals and websites of the Presidential office and foreign and defence ministry were forced down due to the cyber attack.

4

GERMAN CHAMBERS OF INDUSTRY AND COMMERCE SUFFERED A CYBER ATTACK

In response to a massive cyber attack, the Association of German Chambers of Industry and Commerce (DIHK) was forced to take down all of its IT systems and turn off digital services, telephones, and email servers. With more than three million members, including firms ranging from small shops to large corporations, DIHK is an alliance of 79 chambers representing companies within the German state.

5

CISCO SUFFERED A MASSIVE DATA BREACH ATTACK BY A RANSOMWARE GANG

The Yanluowang ransomware group infiltrated Cisco’s corporate network in late May and stole internal data, according to a security breach Cisco reported. Through MFA fatigue and a series of voice phishing attacks impersonating trustworthy support companies, the attacker persuaded the Cisco employee to accept MFA push alerts. The threat actors were able to access the VPN in the context of the targeted user after ultimately tricking the victim into accepting one of the MFA alerts.

6

CLOUDFLARE TARGETED BY THE SAME HACKERS BEHIND TWILIO BREACH

Cloudflare claims that some of its employees’ credentials were also stolen in an SMS phishing attack identical to the one that led to the breach of Twilio’s network last week. They stated that at least 76 workers and their families had received texts on their personal and work phones. Even though the attackers gained access to the accounts of Cloudflare workers, they were unable to compromise the company’s systems

7

LOCKBIT RANSOMWARE CLAIMED ATTACK ON SECURITY GIANT ENTRUST

In June, the LockBit ransomware group claimed responsibility for the strike against Entrust (a digital security giant). Entrust revealed a cyberattack in June of this year in which some of its data was compromised from its internal systems. Entrust informed its clients that they are investigating the incident and will get back to them with further details

8

FAKE CLOUDFLARE DDOS ALERTS COMPROMISE WORDPRESS WEBSITES

WordPress sites were compromised by fake Cloudflare DDoS alerts Pushing Malware Infections. Threat actors used WordPress websites to propagate malware that installs the RaccoonStealer password-stealing Trojan and the NetSupport RAT by displaying fake Cloudflare DDoS protection pages.