Universidade do vale do Itajaí – UNIVALI

Nome: Mariana Ferreira

Disciplina: Segurança de Sistemas Computacionais

Ataque DDoS direcionado à Dyn

Em outubro de 2016, um ataque DDoS atingiu a Dyn, um provedor de DNS, causando a queda e instabilidade de sites como Airbnb, Netflix, Amazon, Reddit, GitHub, entre outros. Os invasores utilizaram o botnet mirai, composto por dispositivos IoT comprometidos. Entre os alvos mais comuns estão câmeras de segurança, TVs inteligentes, rádios e impressoras.

* Quais vulnerabilidades foram exploradas?

O ataque explorou principalmente vulnerabilidades em dispositivos IoT, que frequentemente vinham com credenciais padrão fracas. Muitos desses dispositivos possuíam um usuário e senha padrão que não eram alterados pelos usuários. Além disso, a ausência de mecanismos de proteção contra botnets tornava a maioria dos dispositivos IoT ainda mais vulneráveis.

* Quais ativos foram comprometidos?

Os Dispositivos IoT infectados, como câmeras de segurança e roteadores, empresas de serviços online para os quais a Dyn prestava serviço, como Twitter, Netflix, GitHub, Reddit, entre outros, além de várias pessoas que dependiam desses serviços e ficaram sem acesso por várias horas.

* Quais propriedades de segurança foram violadas?

Disponibilidade: O ataque DDoS tornou os serviços DNS da Dyn indisponíveis.

Referências:

<https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/>

<https://bluecatnetworks.com/blog/bluecat-director-cybersecurity-solutions-dyn/#:~:text=The%20Dyn%20Attack%20Explained&text=This%20attack%20used%20a%20massive,unavailable%20for%20an%20extended%20period>.