Cybraics Identifies Phishing and Ransomware From “Legitimate” Websites

Challenges

- Signature-based web proxy servers are often outdated
- Legitimate domains often get purchased by cyber squatters and used for malicious intent

Existing Security Tools:

- IDS/IPS, Threat Intelligence, SIEM, Advanced Threat Detection

Results

- Identified users visiting legitimate websites redirecting to phishing and ransomware sites

Background

The healthcare provider has a dedicated security operations team and has implemented several advanced security measures, including IDS/IPS, SIEM, threat intelligence, and a threat detection service that reviews security logs and hunts for threats. They have been proactive in implementing rules and policies based on blacklists to block access to known malicious sites and IP addresses.

What We Found:

Analyzing firewall, DNS, and web proxy logs to correlate events and traffic, the nLighten platform identified suspected malicious web traffic between hosts on the customer’s network and legitimate external domains. The investigation revealed that several devices and users on the customer’s network were browsing to domains previously registered to legitimate medical companies, ostensibly searching for information related to their work function. Unbeknownst to the users, these domains had expired, and cyber squatters had registered them to serve malicious content. Over a dozen different domains became affected, and those that browsed these sites were redirected to spam sites. While many of these spam sites are benign, primarily used for ad and click-fraud, some contain malicious code, redirecting users to phishing and ransomware sites.

These compromised domains implement a clever technique found in recent malware campaigns using Angler EK where the IPs and sub-domains constantly change, often using tens of thousands of sub-domains, maintaining the same name for only a few brief minutes. It then becomes very difficult to identify the domains and IP’s and add them to a blacklist, and virtually impossible for traditional tools to detect and block them within that timeframe of activity.

Result:

The nLighten platform detected this malicious activity despite the fact that users were communicating with domains previously identified as trusted. By exposing this activity, the customer was able to respond by blocking access to these destinations, protecting their customers from sophisticated phishing campaigns and ransomware payloads.