UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00059

PARKED DOMAINS & TYPOSQUATTING

DATE ISSUED: 2nd November 2020

IMPACT	[✓ LOW]	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Using a Parked Domain as an alias, attackers are impersonating well known brand to direct victims to malicious or advertising websites.

BREAKDOWN

Search engines can be a great tool for locating a website you're after using keywords, but malicious actors have been using this to their advantage. Attackers are taking the names of popular brands and creating impersonation websites to distribute malware or grayware or simply bombard the user with advertising to create impressions. By simply adding a different suffix or prefix for a parked domain or making the URL a very close match to the real site for typosquatting, the website, at first glance, appears to be legitimate. For example, when using a search engine and typing in a key word, the first result may show a '.net' suffix, rather than the legitimate '.com' website first, prompting users to click on the first result and be directed to a malicious or advertising site. An example of typosquatting was seen to impersonate Comcast's xfinity.com website using 'xifinity' to fool victims. A surge in these kinds of attacks has been seen with the lead up to the elections claiming to be representative of the parties running in the election. Another notable attack was the impersonation of the McAfee website where the landing page led users to believe their machine was infected as their subscription had expired and prompted them to renew. When the user proceeded, they were in face redirected to the legitimate McAfee download page, and it is suspected the attackers were using the former page to steal advertising revenue. 27,000 new parked domains have been discovered daily on average by Palo Alto with 5million total in the past 6 months. 1% were deemed malicious, 3% fit into the 'not safe for work' category and a further 31% appeared suspicious.

REMEDIATION STEPS

- Wherever possible, type the URL into the address search bar of your browser in full
- Keep track of parked domains and prevent access to them using your URL filtering

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/xfinity-mcafee-brands-abused-parked-domains/160698/