Illicit Brand Impersonation: A Threat Hunting Approach

By Tom Vager

The persistent use of brand impersonation by opportunistic and sophisticated threat actors for illicit activities like credential phishing and malware

Conclusion

Here is a list of Domains/URLs which contain our Kimsuky

While beta testing NetIoc with this rule, the le triggered across many unreported Kimsuky controlled URLs, and can also be found going back mult

Passing in our

and acting as an input for credential theft functionality.

component we call ReconShark. In some of the malicious URLs, we can see the actor making use of a

might expect, depending on the attacker and campaign of course.

very simple rule monitoring for that same tracker.

Earlier this month Malwarebytes

sites.

One useful way to identify automated and often large-scale phishing campaign infrastructure is through monitoring and alerting on actor specic ch

Reused Characteristics of Infrastructure – Commodity Targeting

AWs is just one example, threat hunters could instead use this for less common pages of value like download sites or internal intranet employee log

content, and images. If the VirusTotal scanner catches it fast enough, we can track down some commodity activity with this in mind.

solutions for network data detection opportunities.

Let's explore some examples of opportunistic and targeted threat actors impersonating trusted brands and

while tracking more capable and often state-sponsored threat actors, we continually observe brands being impersonated for illicit use, including cr

Since the start of 2023, brand impersonation has become the center of many questions we receive from everyday network defenders. While at the

Don't miss OneCon23! SentinelOne's annual Customer Conference.

B l o g