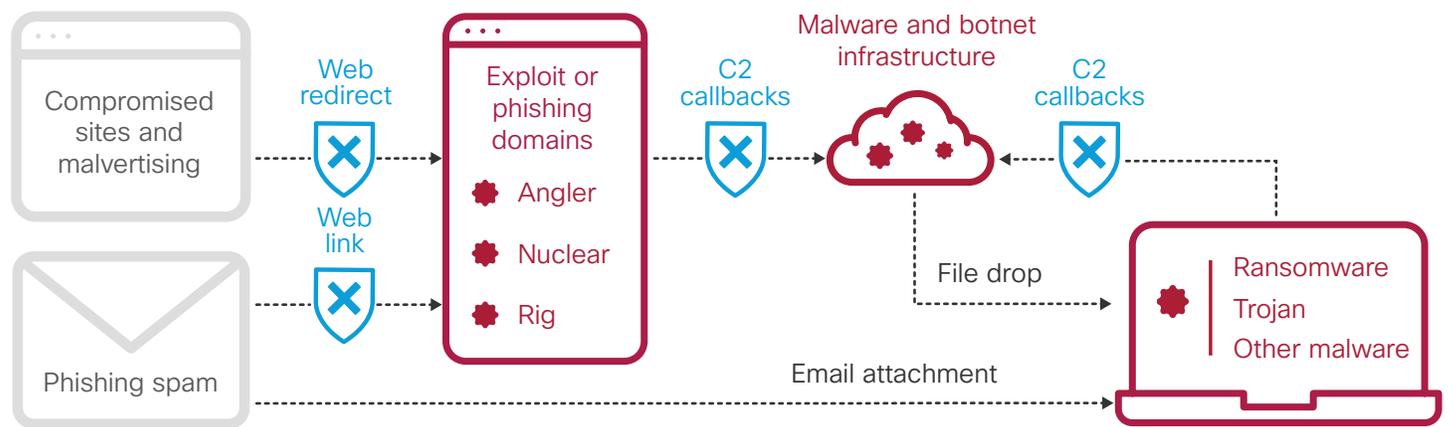


Waste less time fighting ransomware attacks.

Does Cisco Umbrella for MSPs block ransomware?

This is one of the most common questions that we hear from customers. In reality, the answer for any security provider – including Cisco – is seldom an absolute “yes” or “no.” It really depends on how each variant arrives onto your systems, as well as its order of operations for encrypting data for ransom. However, with Cisco you can significantly reduce the number of ransomware infections across your organization.

Prevent and contain ransomware with Cisco Umbrella



Phases of ransomware attacks

Attackers have many ways to initiate an attack—everything from common malvertising and phishing methods to sophisticated thumbdrive drop tactics. The infections can begin when users click on links in phishing emails or if malicious ads or compromised sites redirect users to domains hosting exploit kits (e.g. ‘Angler,’ ‘Zeus,’ ‘Nuclear,’ etc.). Exploit kits can also be delivered via email attachments or infected thumbdrives. Interestingly, this initial payload is not the ransomware.

Assuming the initial payload successfully exploits a system, it analyzes its environment (e.g. OS, unpatched applications) to select an effective ransomware variant. At this point, a callback is made to a ransomware drop host to retrieve the private keys needed to encrypt the endpoint. Most popular exploit kits have to resolve a domain name to an IP address to initiate the callback.

Although variants of ransomware behave differently – for example, SamSam uses a built-in encryption key that doesn’t require a C2 callback and other variants use Tor-based Onion Routing or IP-only callbacks that avoid DNS – there are many ways that Cisco can help.

Cisco Umbrella for MSPs

Cisco Umbrella is a cloud security platform that is built into the foundation of the internet and provides the first line of defense against threats wherever users go. In the case of the initial infiltration, Umbrella can block the DNS request before the browser connects to the malicious site – whether the user clicked on a link or if there was a redirect from a compromised site. If Cisco Umbrella flagged the exploit or phishing domain as malicious, then Umbrella would block the connection before the compromise occurs.

Additionally, Umbrella excels at stopping C2 callbacks – over any port or protocol – which can stop the ransomware drop or the C2 callback for the encryption key. Another challenge with ransomware is when an infected device connects to more shared drives and the infection spreads across your organization. With Umbrella, you can immediately pinpoint the source of botnet activity and mitigate further damage.

You might be wondering how we determine what domains and IPs are malicious. Similar to how Amazon learns from shopping patterns to suggest the next purchase, we learn from internet activity patterns from 80+ billion daily DNS requests to identify attacker infrastructure being staged for the next threat. Leveraging statistical models developed by the Umbrella security researchers, we're able to automatically discover, classify, and even predict the callback destinations used by exploit kits, phishing campaigns, and many ransomware variants.

