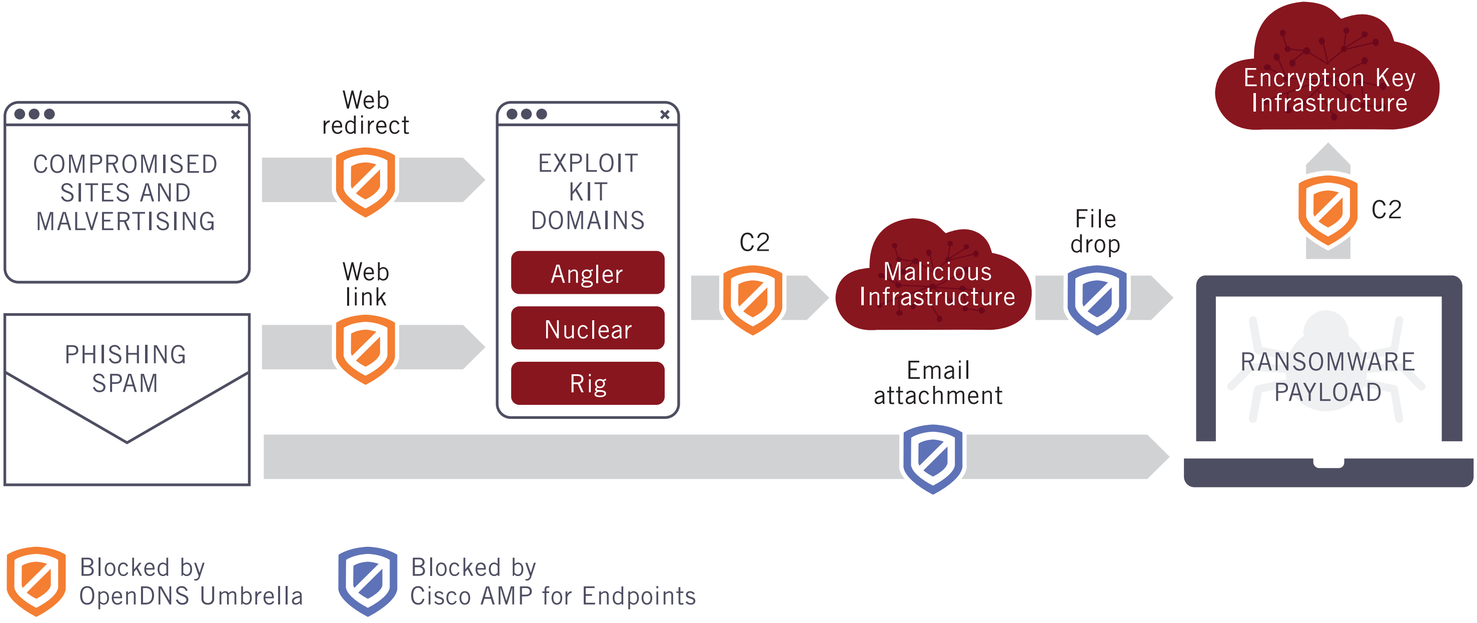
Solution Brief

Waste Less Time Fighting Ransomware Attacks

"DOES OPENDNS BLOCK RANSOMWARE?"

This is one of the most common questions that we hear from customers. In reality, the answer for any security provider — including OpenDNS and 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 OpenDNS and Cisco you can significantly reduce the number of ransomware infections across your organization.

PREVENT AND CONTAIN RANSOMWARE WITH OPENDNS UMBRELLA AND CISCO AMP FOR ENDPOINTS



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.

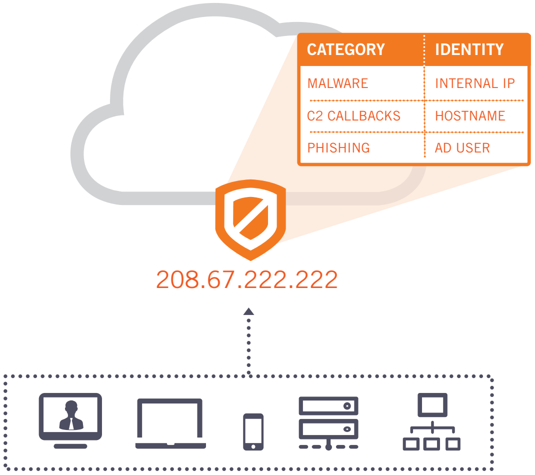
Although variants of ransomware behave differently — for example, CryptoWall uses a built-in encryption key that doesn't require a C2 callback and other variants use Tor-based Onion Routing or IP-only callbacks that avoid DNS — there are many ways that OpenDNS and Cisco can help.

OPENDNS UMBRELLA

OpenDNS Umbrella enforces security at the DNS-layer — protecting devices on and off the corporate network. In the case of the initial infiltration, OpenDNS Umbrella could 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 OpenDNS 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, OpenDNS learns 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 OpenDNS Security Labs team, we're able to automatically discover, classify, and even predict the callback destinations used by exploit kits, phishing campaigns, and many ransomware variants.



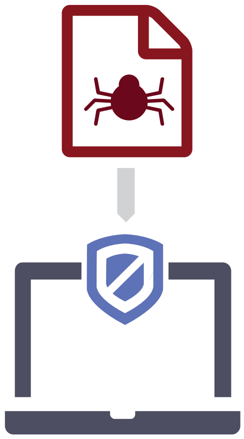
CATEGORY	IDENTITY
MALWARE	INTERNAL IP
C2 CALLBACKS	HOSTNAME
PHISHING	AD USER

DNS-LAYER SECURITY
WITH OPENDNS UMBRELLA

CISCO AMP FOR ENDPOINTS

Cisco Advanced Malware Protection (AMP) for Endpoints provides point-in-time protection against known malware files and uses continuous analysis and retrospective security to detect malware that evades initial inspection. Using a combination of file signatures, file reputation, behavioral indicators, and sandboxing, AMP can stop the initial exploit kit from executing on the endpoint and can also stop the execution of the ransomware file and remove it.

In addition, AMP continuously analyzes and records all file activity on a system, regardless of file disposition. If at a later date a file behaves suspiciously, AMP retrospectively detects it and alerts your security team. AMP provides a detailed recorded history of the malware's behavior over time, including where and how it entered the network, where else it traveled, and what it's doing. Based on a set policy, AMP can then automatically contain and remediate the threat, or enable the security team to manually block and remediate with a few clicks in the console.



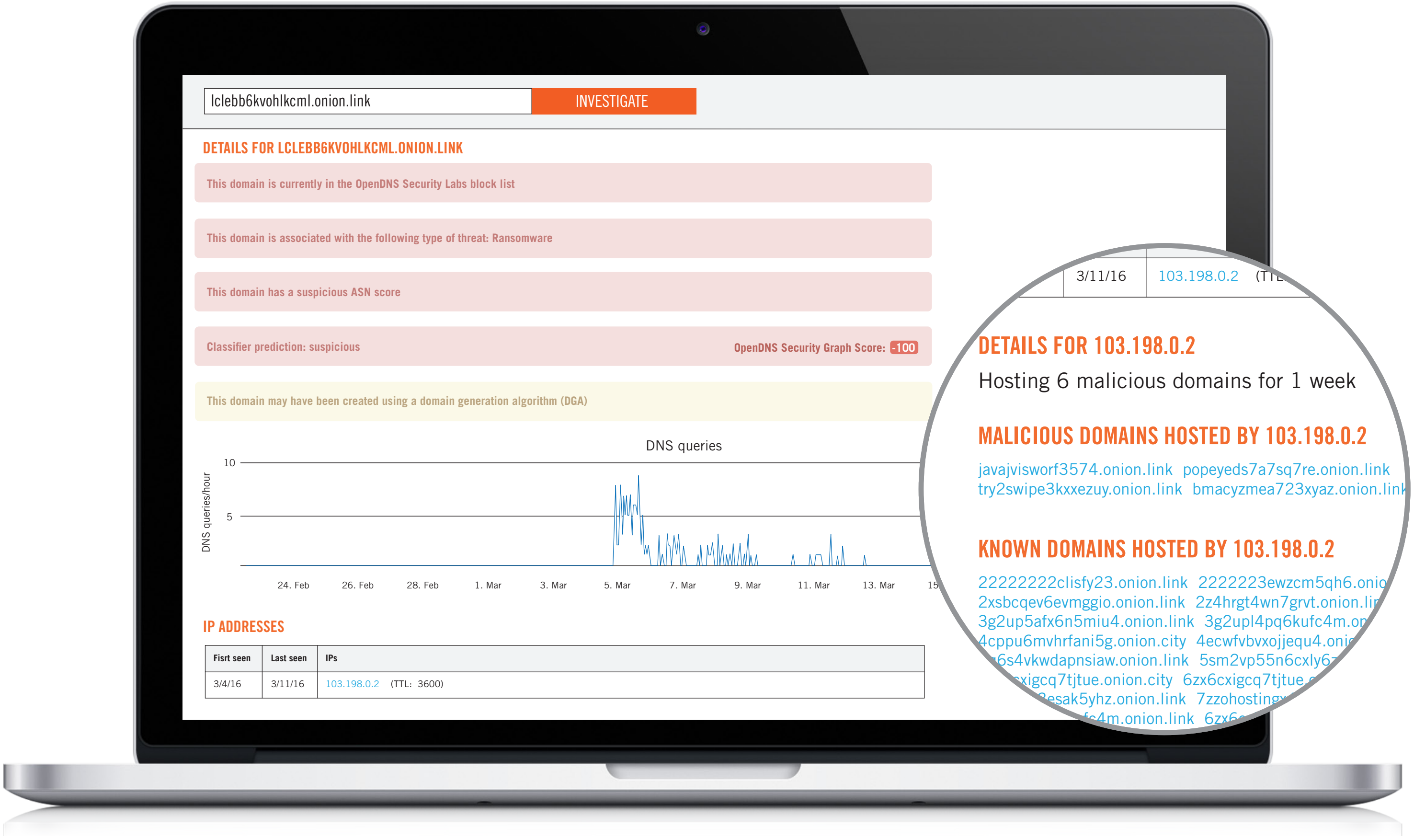
BLOCK RANSOMWARE FILES WITH
CISCO AMP FOR ENDPOINTS

RESEARCHING RANSOMWARE WITH OPENDNS INVESTIGATE

Have you ever wanted to learn more about the infrastructure being used by a ransomware attack? Imagine being able to uncover all of the domains and IPs related to an attack — whether you're in the middle of an incident investigation or proactively hunting and researching potential threats.

OpenDNS Investigate gives you access to all of our threat intelligence about domains and IPs, and can be used to map out the Internet infrastructure that attackers are using to launch current and future attacks. Using Investigate, security teams can not only immediately validate malicious domains and IPs, but also pivot on different data points to build out a view of other related infrastructure used in attacks.

For example, say you start with one IOC (e.g. a Tor proxy domain). Using Investigate, you can first determine that it's a malicious domain currently being blocked by OpenDNS and is associated with a ransomware attack — plus other details including WHOIS record data, a graph showing the DNS queries per hour, and much more. You can then pivot on the IP address and uncover all of the other domains being hosted by the same network. In a matter of a few clicks, OpenDNS Investigate gives you a more comprehensive view of the Internet infrastructure associated with ransomware attacks.



DETAILS FOR LCLEBB6KVOHLKCML.ONION.LINK

This domain is currently in the OpenDNS Security Labs block list

This domain is associated with the following type of threat: Ransomware

This domain has a suspicious ASN score

Classifier prediction: suspicious — OpenDNS Security Graph Score: -100

This domain may have been created using a domain generation algorithm (DGA)

IP ADDRESSES

First seen	Last seen	IPs
3/4/16	3/11/16	103.198.0.2 (TTL: 3600)

	3/11/16	103.198.0.2 (TTL

DETAILS FOR 103.198.0.2

Hosting 6 malicious domains for 1 week

MALICIOUS DOMAINS HOSTED BY 103.198.0.2

javajvisworf3574.onion.link popeyeds7a7sq7re.onion.link
try2swipe3kxxezuy.onion.link bmacyzmea723xyaz.onion.link

KNOWN DOMAINS HOSTED BY 103.198.0.2

22222222clisfy23.onion.link 2222223ewzcm5qh6.onio
2xsbcqev6evmggio.onion.link 2z4hrgt4wn7grvt.onion.li
3g2up5afx6n5miu4.onion.link 3g2upl4pq6kufc4m.on
4cppu6mvhrfani5g.onion.city 4ecwfvbvxojjequ4.onio
6s4vkwdapnsiaw.onion.link 5sm2vp55n6cxly6
xigcq7tjtue.onion.city 6zx6cxigcq7tjtue.
esak5yhz.onion.link 7zzohosting
fc4m.onion.link 6zx6

OpenDNS

OpenDNS is
now part of Cisco.

For a free trial or more sales information, contact our team:

1-877-811-2367 | sales@opendns.com | www.opendns.com