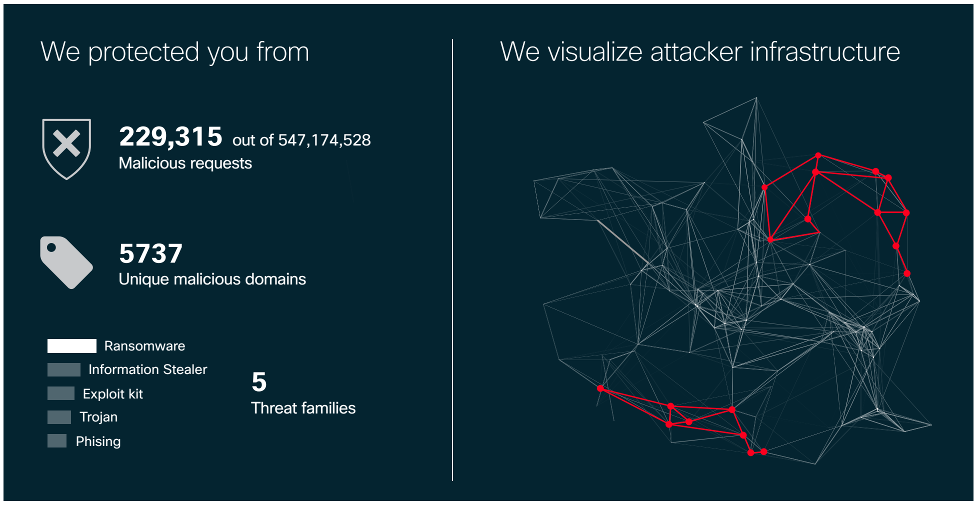
Cisco Umbrella

SOLUTION BRIEF

# Post-trial Umbrella Security Report: Uncover malicious activity over all ports

## See and learn how we protect your enterprise

With this free report, available at the end of your trial, you not only see which threats were blocked and devices are infected, but you learn how Umbrella discovered the attack. Visualizations correlate your local activity with Umbrella's global visibility of attacker infrastructures to show you when and where we protected you. Short videos with Umbrella security researchers reveal the techniques that discover, and often predict, these attacks. For example, a single ransomware domain seen in your local activity is correlated with related domains, IPs, and malware derived from 100B+ daily internet requests and 1.5M+ daily malware samples. Unlike a static executive summary, one of our system engineers will walk your team through an interactive data portal to expand your knowledge about the different threat families and specific attacks operating inside your enterprise environment.



We protected you from

**229,315** out of 547,174,528
Malicious requests

**5737**
Unique malicious domains

- Ransomware
- Information Stealer
- Exploit kit
- Trojan
- Phising

**5**
Threat families

We visualize attacker infrastructure

## Proof of value across your entire enterprise

Most security products pose too much risk or complexity to deploy across your full production network during a trial. If your evaluation has a very limited deployment, the security report fails to really answer:

"How effective is this solution?"

"How does it compare (or add) to my current security stack?"

"Does it deliver great time-to-value?"

With Cisco Umbrella, you can gain enforcement and visibility in minutes across all ports and protocols, on and off network. All you need to do is point DNS traffic to the Umbrella global network. By leveraging DNS—the foundation of the internet—you can safely evaluate how well Umbrella protects your enterprise against malicious activity.

### Minimum requirements

Forward DNS traffic to the Umbrella global network for 14 or more days.

Just change one IP address per network. No other changes to your network or endpoints are required. And your internal domains and DNS servers will not be impacted. Umbrella's recursive DNS service is one of the most reliable and fastest in the world. Your network team and employees will thank you!

View a live sample report:
security-report.umbrella.com

### Attacker infrastructures

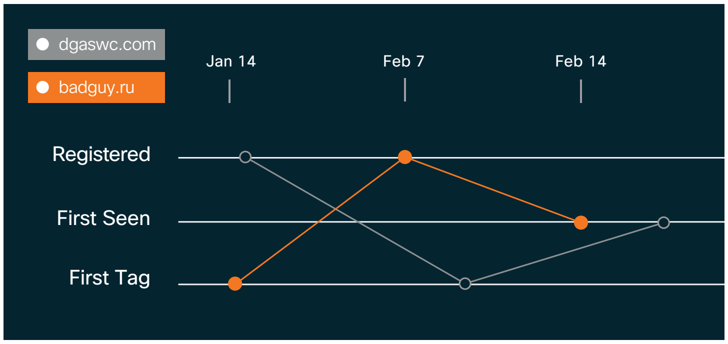
Modern attacks rely on hosting infrastructure in multiple countries and autonomous systems (AS) across the internet. These complex and constantly evolving systems are built from tens to thousands of domains and IPs—even entire ASNs—to stay ahead of traditional reputation systems. Cisco Umbrella security researchers apply statistical and machine learning models to diverse, global data sets for automated discovery of where these infrastructures are being staged—before attacks launch.

> *"It took less than ten minutes for us to point our DNS traffic to the Global Network. We could protect our remote offices around the world in less than an hour and a half."*
>
> Mark Arnold, Director of Information Security, PTC *(read more at cs.co/ptc-umbrella)*

# An Umbrella expert will help you...

### Determine when your activity was first tagged as malicious and whether Umbrella predicted it?

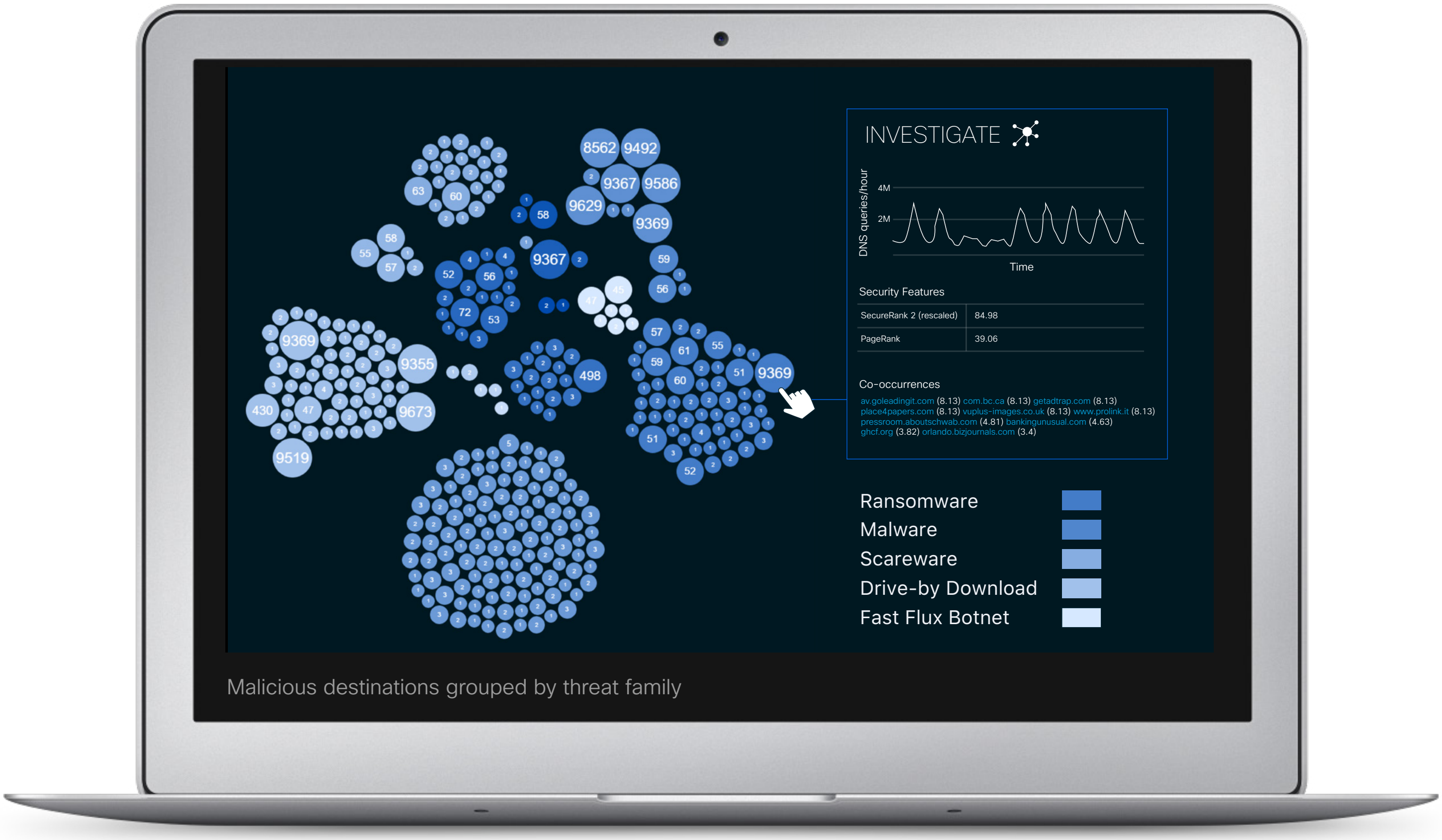
Using statistical and machine learning models, Umbrella can tag domains as being malicious before they're even registered or seen by one of Umbrella's 85M+ active daily users. In this example, one of the malicious domains was predicted three weeks in advance! For malicious activity seen during your trial, the report analyzes the evolution of the threat by correlating DNS queries, WHOIS records, and other data sources to identify attacker infrastructures.



Domain tagged as malicious weeks before registered

### Investigate the threats you're most concerned about impacting your enterprise, such as ransomware.

For ease of use, Umbrella's policies group threats as malware, C2 callbacks (a.k.a. botnets), and phishing. But Umbrella actually classifies up to 20 granular threat families, which are unveiled in this report. Unique malicious domains requested by your devices, each represented as a bubble, are visually grouped by threat. The size of each bubble depends on your volume of requests for that domain. With a simple click, all intelligence related to this domain is unveiled in the Umbrella Investigate Console. Your Umbrella expert will help you select several domains to investigate to reveal co-occurrences, associated malware samples, more domains registered by the same actor or hosted on the same nameserver, all IP addresses mapped to this domain over the last three months, and many feature scores.



Security Features

| | |
|---|---|
| SecureRank 2 (rescaled) | 84.98 |
| PageRank | 39.06 |

Co-occurrences

av.goleadingit.com (8.13) com.bc.ca (8.13) getadtrap.com (8.13)
place4papers.com (8.13) vuplus-images.co.uk (8.13) www.prolink.it (8.13)
pressroom.aboutschwab.com (4.81) bankingunusual.com (4.63)
ghcf.org (3.82) orlando.bizjournals.com (3.4)

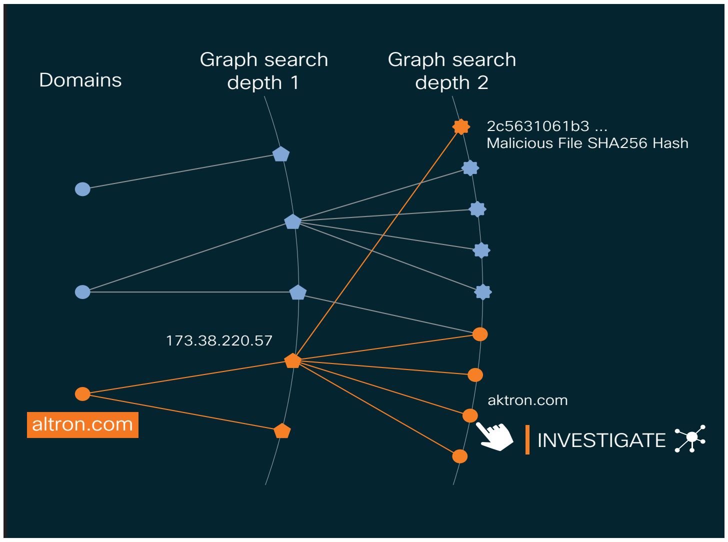
| | |
|---|---|
| Ransomware | ▇ |
| Malware | ▇ |
| Scareware | ▇ |
| Drive-by Download | ▇ |
| Fast Flux Botnet | ▇ |

Malicious destinations grouped by threat family

# An Umbrella expert will help you...

**Trace relationships between your activity and attackers to learn more about the threat.**

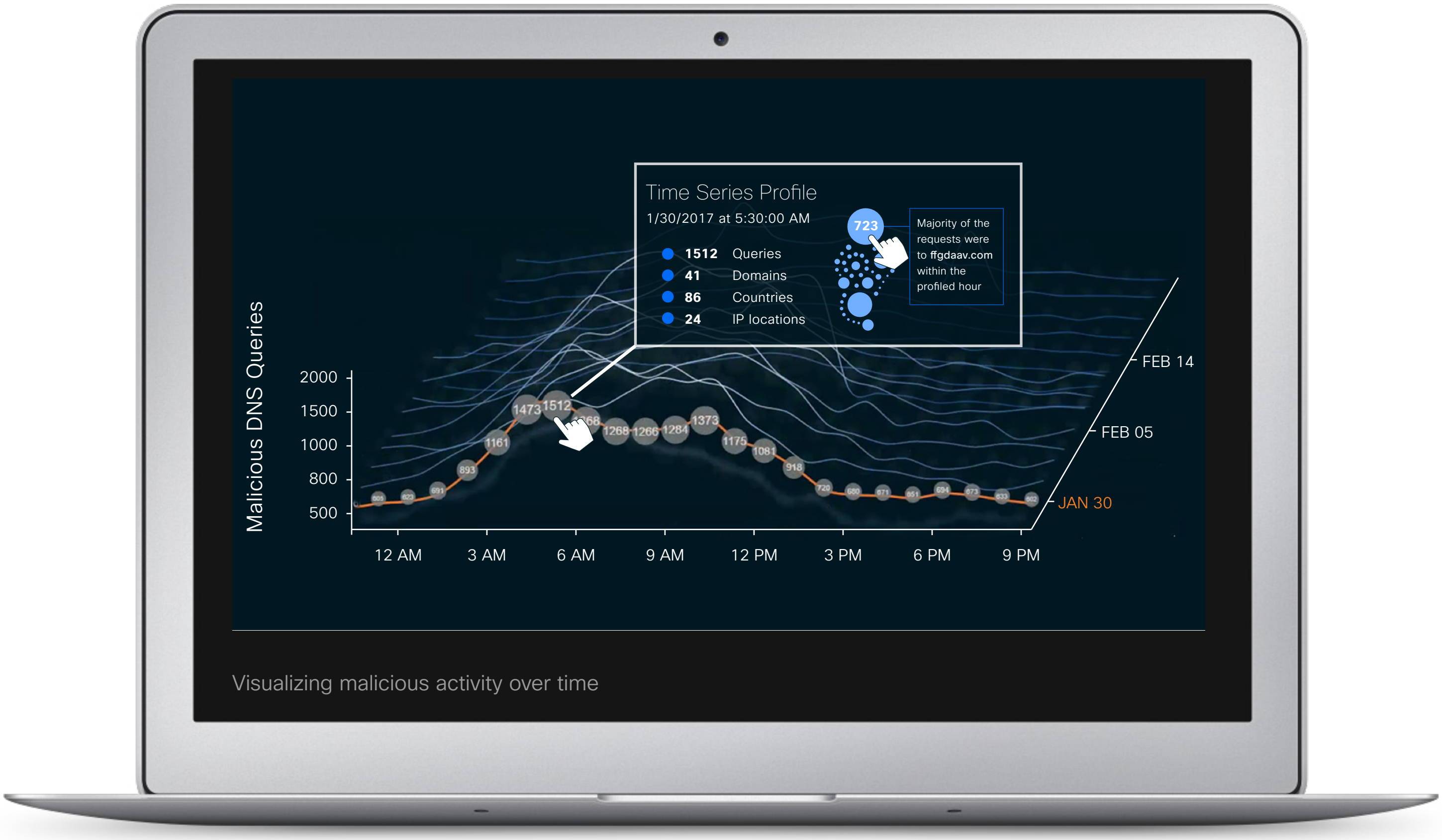
Umbrella continuously graphs the relationships between 2M+ live events per second and 11B+ historical events to track the evolution of attacker infrastructures. Based on your malicious activity and the report's algorithms, a partial view of this massive graph is revealed. For example, several domains requested by your users are related to IPs, email addresses, and even malware files associated with the same threat. This context helps you understand how Umbrella discovered the domains. Beyond just DNS, events are gathered from BGP routes, WHOIS records, and Cisco's sandbox. In particular, the sandbox (a.k.a. AMP Threat Grid) leverages 1.6M+ global sensors to detonate 1.5M+ malware files daily. By observing behaviors including callbacks to domains or IPs, the report shows you what malicious activity could occur if these destinations are not blocked.



Exploit kit infrastructure mapped

**Spot increased malicious activity–does it coincide with a newly infected device or launched attack?**

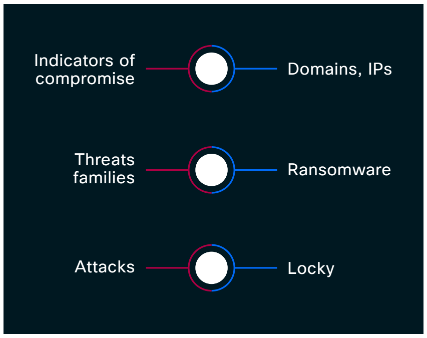
During your trial, it's common to have too many malicious requests to evaluate each one. Time series profiling helps you quickly spot days or hours with increased activity. With a simple click, the report zooms in to show which destinations your devices attempted to connect to. Quickly compare your local activity vs. what Umbrella sees globally. Learn which IPs host these malicious domains, where IPs are located and from which countries malicious domains are accessed. The report visualizes these insights with an interactive user experience to make it easier to prove the value of Cisco Umbrella.



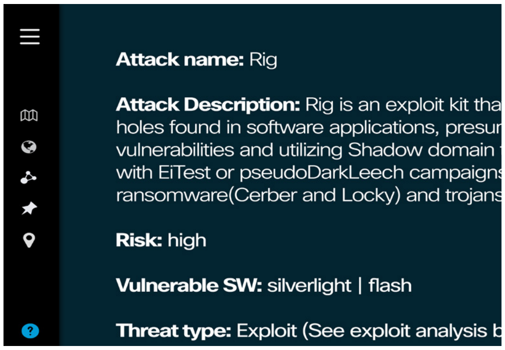
Visualizing malicious activity over time

## Learn your exposure to specific attacks

While Cisco Umbrella can enforce security at the DNS-, IP-, and HTTP/S-layer, this report does not require that blocking is enabled and only monitors your DNS activity. Any malicious domains requested and IPs resolved are indicators of compromise (IOC). This report, along with your Umbrella expert, will help you associate these IOCs to threat families and specific attacks (e.g. Locky) that exposed your enterprise to risk. Learn about each attacks' objectives, lateral movement and communication tactics using the intelligence gathered by Umbrella security researchers and Cisco Talos.



**Example attack details include:**



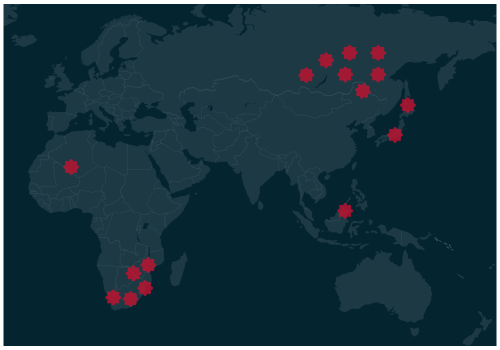
**Attack name:** Rig

**Attack Description:** Rig is an exploit kit tha holes found in software applications, presur vulnerabilities and utilizing Shadow domain with EiTest or pseudoDarkLeech campaigns ransomware(Cerber and Locky) and trojans

**Risk:** high

**Vulnerable SW:** silverlight | flash

**Threat type:** Exploit (See exploit analysis b



### Risk analysis

Umbrella security researchers share their knowledge about how the attack spreads (e.g. email attachments), which software vulnerabilities (e.g. Flash) it exploits, how it maintains command and control (e.g. DGA), what data the attacker collects from infected devices, and other relevant insights.

### Geo-location analysis

The report leverages GeoIP data to map the server locations hosting the attacker infrastructure. For instance, you'll often see attackers using a country-code top-level domain (e.g. FR) that does not match the IP address locations (e.g. China and South Africa).

## But first, you need to start your instant trial

- Visit signup.umbrella.com to provision your free Cisco Umbrella Insights package in seconds.
- At any time, point your DNS to 208.67.222.222 for the most reliable, fastest internet connectivity. Learn all 10 reasons why you should by visiting cs.co/10ForDNS.
- Gain instant visibility and optionally enforce security policies, by adding your DNS traffic egress IP addresses in the Umbrella dashboard.
- If you meet the minimum requirements, contact an Umbrella expert to request the Umbrella Security Report. Your trial will also be upgraded to Cisco Umbrella Platform, which includes the Investigate Console.

### Cisco Umbrella—the industry's first Secure Internet Gateway (SIG)

The cloud-delivered platform protects employees both on and off the corporate network. It stops threats over all ports and protocols with the broadest coverage of malicious destinations and files.

Cisco Umbrella