Cisco Umbrella

Umbrella Security Report

Prepared For: [redacted]

Prepared On: 10/04/2021


We See Data

Patterns of guilt

NLP Rank

Spike Rank

Live DGA Detection

Live DGA Prediction

Sender Rank

Guilt by inference

Co-occurrence model

Geo-Location model

Secure rank

NLP Rank

Guilt by association

Predictive IP Space Modeling

Passive DNS & WHOIS Correlation


Patient Zero
4
Target expansion
5
Wide-scale expansion
6
Defense signatures built
7
Attack kill chain
Reconnaissance and infrastructure setup
Domain registration, IP, ASN Intel
Monitor adaption based on results
We deliver the value to you

* Background map provides a view into the geographical locations of the malicious domains found in your network

We protect you from

176,835 (of 49,232,845) Malicious requests

63 Top Malicious Domains

166 Requests to **21** Newly Seen Domains

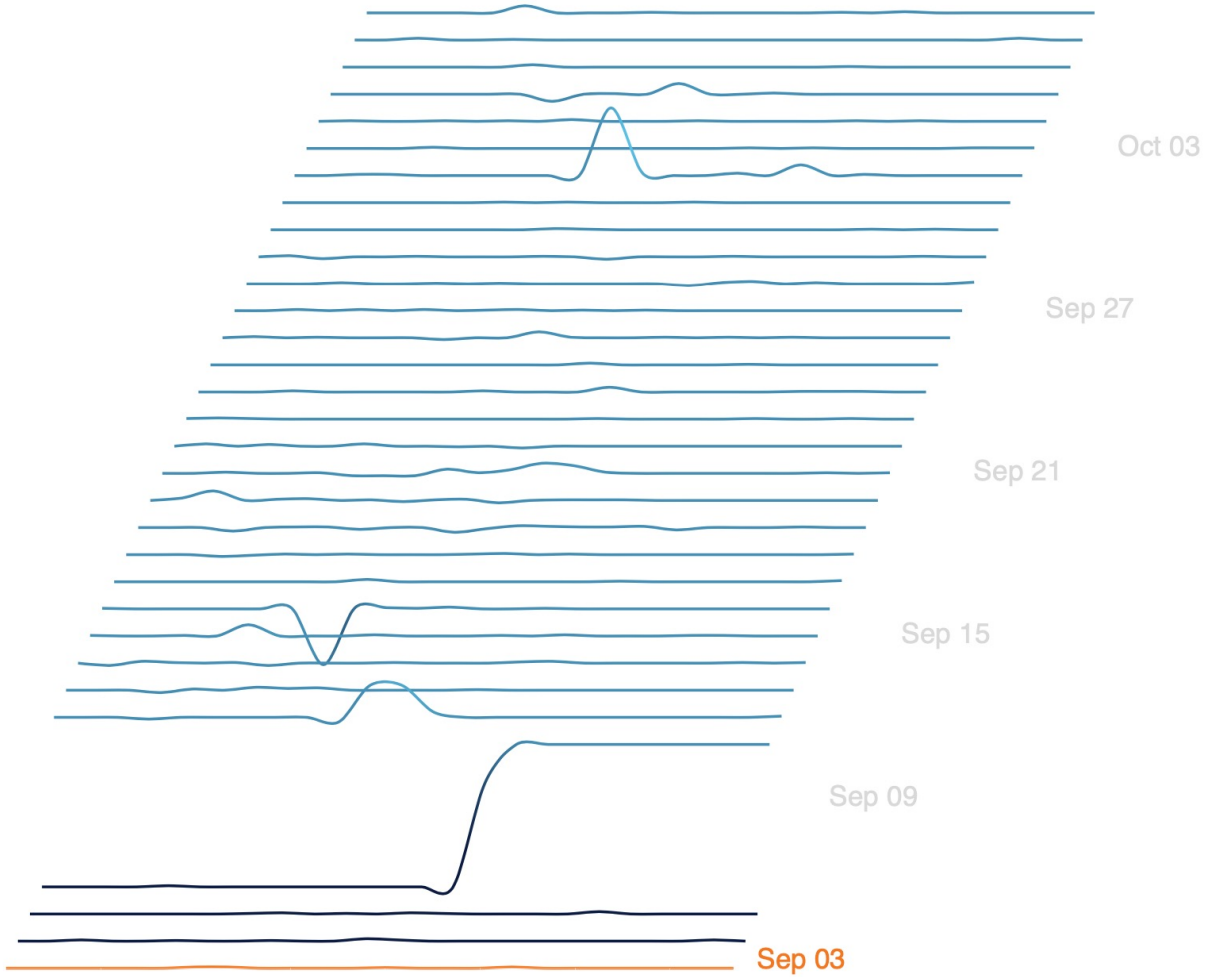
71 Requests to **17** Cryptomining Domains

4 Threat types

Malicious Activity

An interactive timeline of malicious activity on your network between 9/3/2021 and 10/3/2021 arranged by day is shown to the right.

At 354 queries 10AM 9/27/2021 had the largest number of requests in the observed 744 hour period.



Newly Seen Domains

Newly Seen Domains (NSD) is a security setting to block domains that are newly seen in our DNS logs that we have never seen lookups for in the past. Once a NSD is first seen, it's added to a list where eventually it will expire and no longer be 'newly seen'. New domains are often 'spun-up' as part of new malware campaigns. However, a significant portion of the domains that are categorized as 'newly seen' will not, in fact, be malicious and detections of good domains are expected to occur with this security category.

166 Requests to **21** Newly Seen Domains

Domain	Other Categories	First Seen by Umbrella	Number of Queries
1x-xredbet7709390.top		9/17/2021 12:49 PM	2
ads-website.ytsservice.com		9/27/2021 12:23 PM	2
api-v3.thaiwater.net	Research/Reference	9/27/2021 1:11 PM	118
api-v3.twindex.com		9/10/2021 7:48 AM	1
api.astro-stuffs.com		9/11/2021 1:42 AM	1
cdn.getsharedstore.com		9/10/2021 7:40 PM	1
cdn10000.koralast.com		9/30/2021 2:45 PM	1
feetmeantype.top		9/7/2021 5:03 PM	2
my-prize-here-i7.live		10/3/2021 3:40 AM	12
playerkm-02.xyz		10/3/2021 12:21 AM	1

Cryptomining

Cryptomining is a security setting that allows you to block identities from accessing known cryptomining pools where miners group together and share resources, or processing power, to better gather and share cryptocurrencies, and from known web cryptomining source code repositories.

71 Requests to 17 Cryptomining domains

Domain	Other Categories	First Seen by Umbrella	Number of Queries
autofaucet.org		9/1/2016 1:58 PM	1
cryptobrowser.site		5/2/2018 1:39 PM	14
download.cryptobrowser.today		11/14/2018 9:52 PM	2
ethprominer.com		5/24/2017 12:06 AM	8
flash-mini.com	Search Engines	4/13/2015 11:05 PM	5
konstantinova.net	Online Trading	9/7/2016 5:31 PM	2
litecoin.host		5/26/2016 5:28 AM	1
mining-forever.com		12/27/2017 10:32 PM	4
raven.cryptotab.net		3/15/2018 2:34 AM	2
saber.so		11/26/2015 11:33 PM	1

DNS Tunneling

DNS Tunneling is a security setting that allows you to block traffic that utilizes the DNS protocol to communicate non-DNS traffic over port 53. DNS Tunneling sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. However, there are also malicious uses.

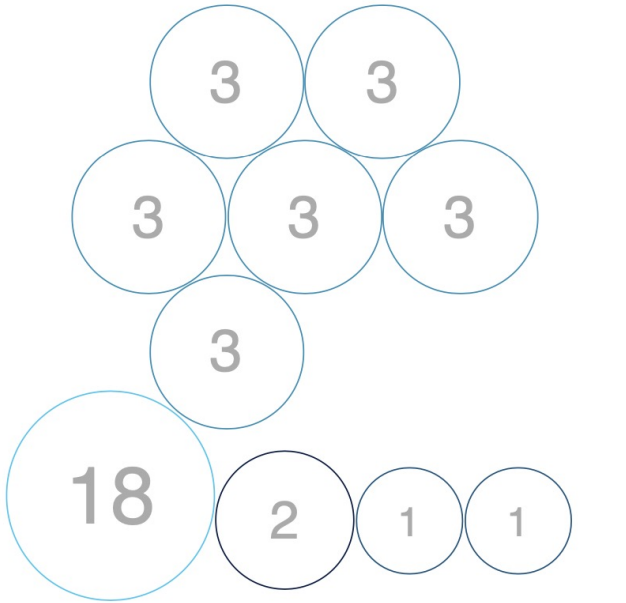
Threat actors can use manipulated DNS requests to exfiltrate data from a compromised system to the attacker's infrastructure. And in some cases, DNS responses are manipulated for C2 callbacks from the attacker's infrastructure to a compromised system. IT Policy avoidance and guest WiFi abuse are also concerns.

We detected no DNS Tunneling requests during your trial period.

Significant Findings

We identified a total of **4** threat types. They are associated with **10** unique domains shown on the right as bubbles.

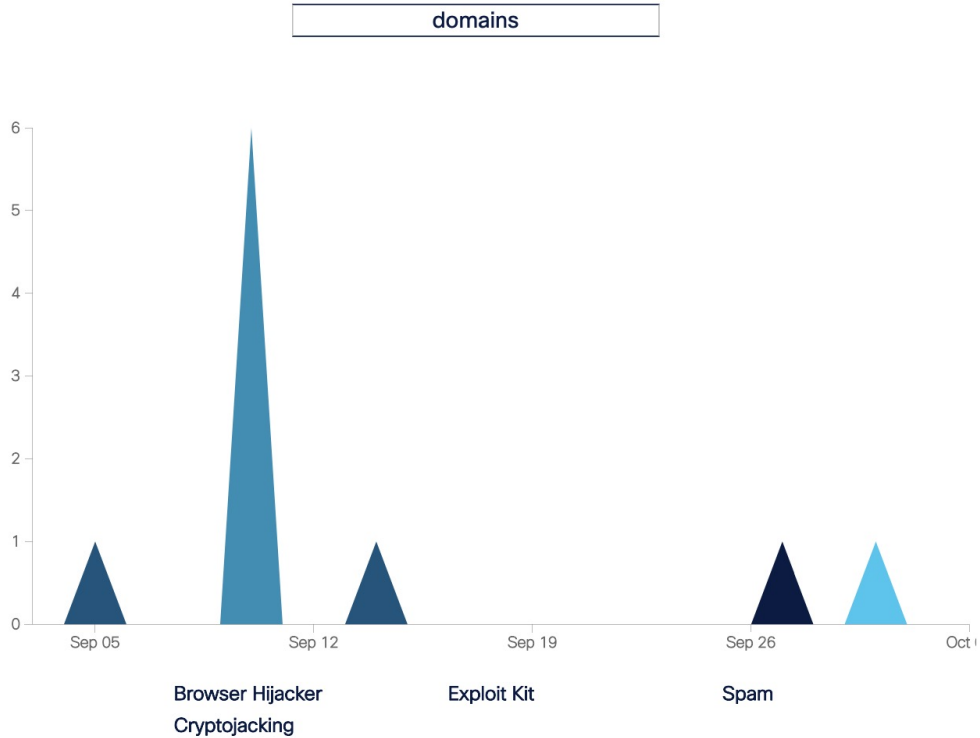
8 domains are associated with widespread and well known attacks. They will be detailed in the next pages of this report.



Significant Findings

This area chart shows how your organization encountered each threat over time.

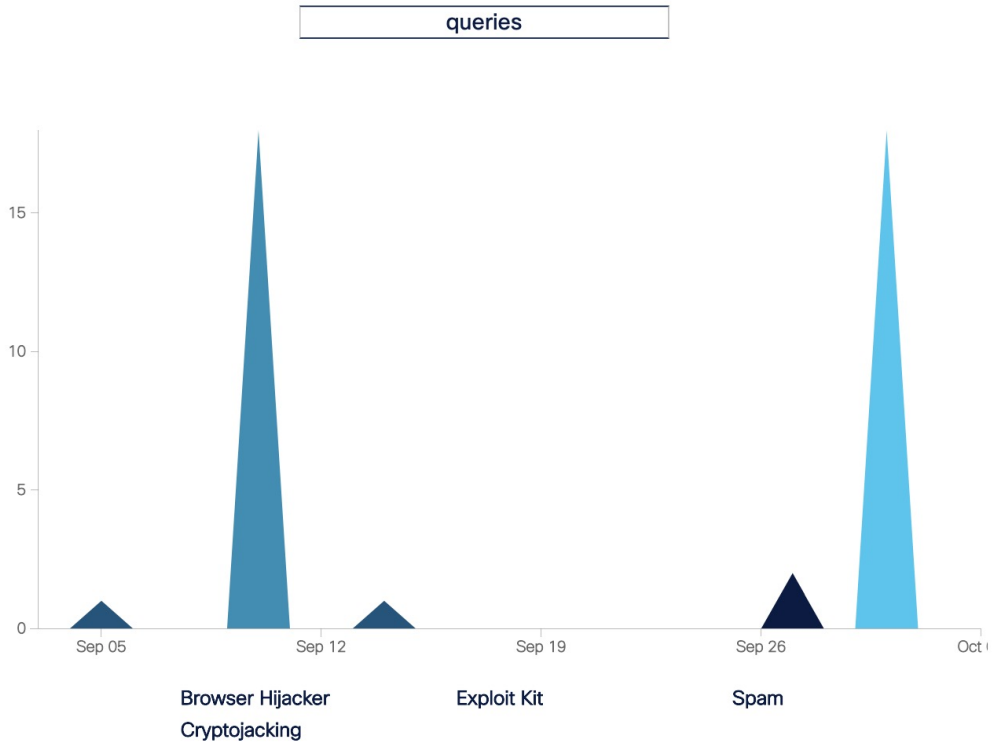
You can view it by number of domains or queries.



Significant Findings

This area chart shows how your organization encountered each threat over time.

You can view it by number of domains or queries.



Exploit Kit

Attackers use Exploit kits to gain control of devices and servers as entry points for malicious payload delivery (e.g. ransomware). Exploits are generally objects (e.g. strings, set of instructions) that a program cannot correctly process and is forced to behave unexpectedly or do operations that are not normally permitted (e.g. install other software). This normal flow disruption is caused by flaws in software code commonly called vulnerabilities. Attackers increase the chances of infection by targeting multiple vulnerabilities - Exploit kits. Exploit kits are delivered over the Internet. Attackers hosts Exploit kits on their own websites or compromised legitimate sites to which users are lurked via URLs in phishing email. This type of attack is called drive-by download.

Exploit Kit

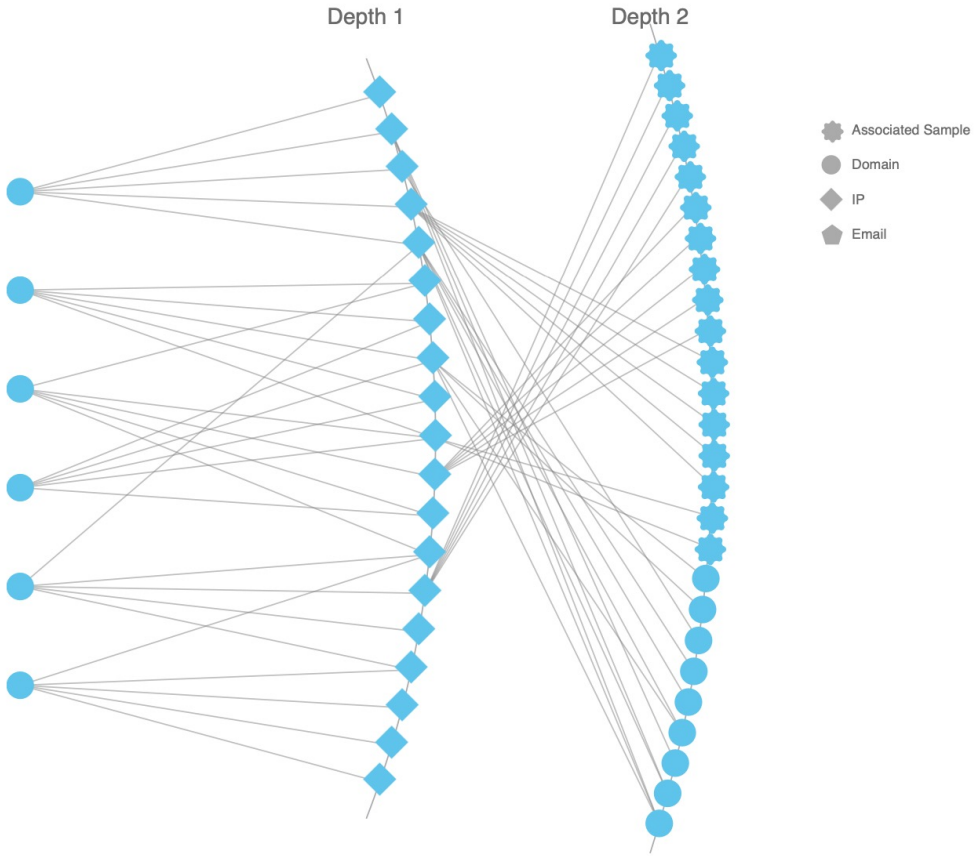
UnderMiner EK

No attack description available.

Domains:

ls8e0th5.wefoundsome.xyz
lpcv8uvh.foundrosysquad.info
f09er35s.redteamshop.info
h1da2yoj.gatedailymirror.info
9ur4zpzx.gatedailymirror.info
e9871xls.redteamshop.info

Infrastructure



We started with our discovered domains and pivoted over Whois and IP data to unveil the network infrastructure behind the attack.

Exploit Kit

UnderMiner EK

No attack description available.

Domains:

ls8e0th5.wefoundsome.xyz
lpcv8uvh.foundrosysquad.info
f09er35s.redteamshop.info
h1da2yoj.gatedailymirror.info
9ur4zpzx.gatedailymirror.info
e9871xls.redteamshop.info

Evolution

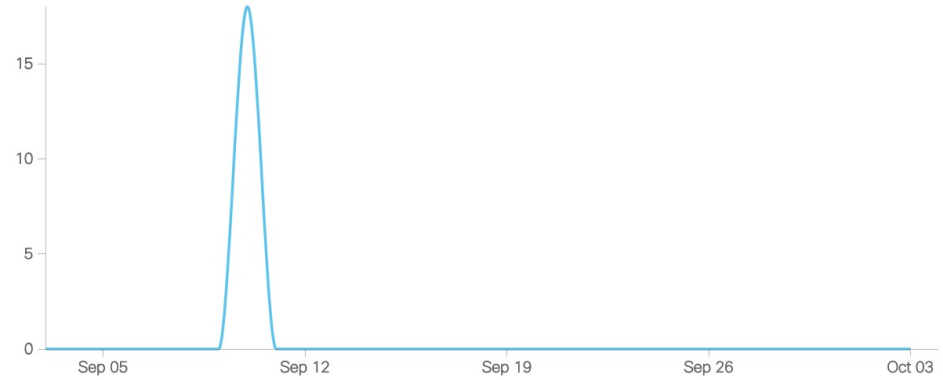
Registered

First Seen

First Tag

Local client traffic over the last month

18 requests made to this attack



Exploit Kit

UnderMiner EK

No attack description available.

Domains:

ls8e0th5.wefoundsome.xyz
lpcv8uvh.foundrosysquad.info
f09er35s.redteamshop.info
h1da2yoj.gatedailymirror.info
9ur4zpzx.gatedailymirror.info
e9871xls.redteamshop.info

Evolution

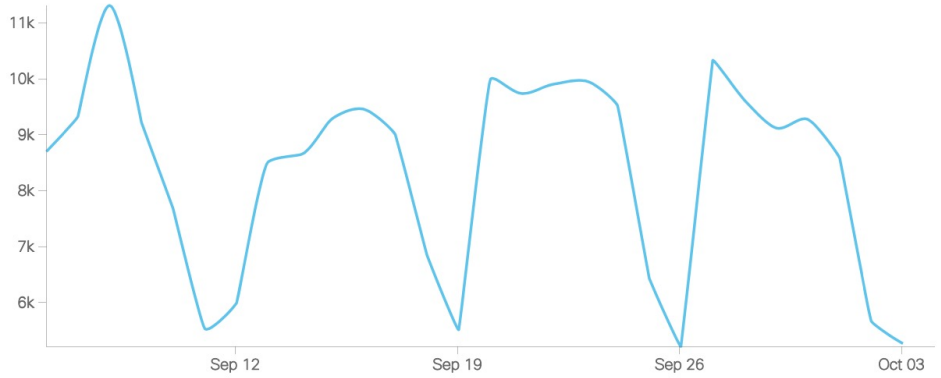
Registered

First Seen

First Tag

Global client traffic over the last month

233691 requests made to this attack



Exploit Kit

UnderMiner EK

No attack description available.

Domains:

ls8e0th5.wefoundsome.xyz
lpcv8uvh.foundrosysquad.info
f09er35s.redteamshop.info
h1da2yoj.gatedailymirror.info
9ur4zpzx.gatedailymirror.info
e9871xls.redteamshop.info

Geolocation

This map provides a geographical view of this attack, based on Maxmind GeoIP data.


CISCO
SECURE