The Fight against Hive Ransomware May Not Be Done as Yet-Unidentified Artifacts Show

Table of Contents

Executive Report

The Hive Ransomware Group has had more than 1,500 victims across more than 80 countries worldwide. They attacked hospitals, school districts, financial firms, and critical infrastructure until the U.S. Department of Justice (DOJ) disrupted their operations. Have we seen the fall of the group's entire infrastructure?

Our indicator of compromise (IoC) expansion analysis found more digital breadcrumbs, including:

- Six IP address resolutions of the domains identified as IoCs
- 936 domains that shared the IoCs' IP hosts, six of which turned out to be malicious
- 28 domains that contained the string ***privatlab*** akin to two of the IoCs, one of which was deemed malicious

Following the Digital Trail Hive Left Behind

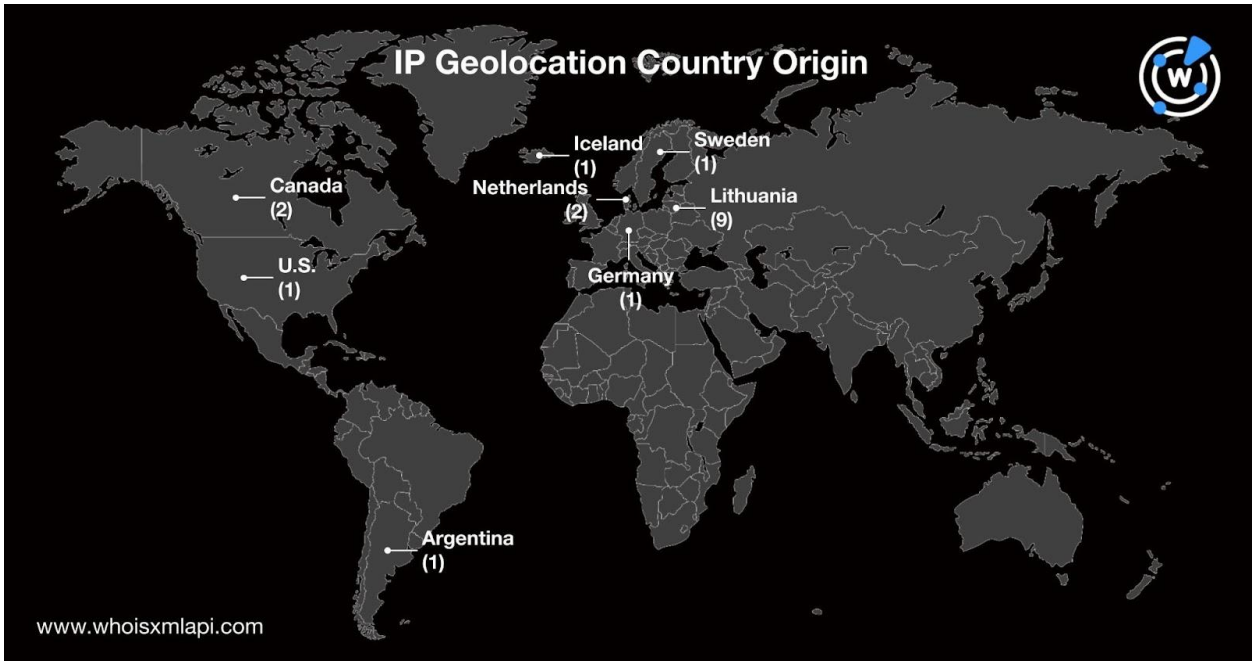
Our expansion analysis began by obtaining a list of Hive ransomware IoCs from AlienVault, which included six domains and 19 IP addresses, namely:

- swhw71un[.]pw
- r77vh0[.]pw
- d6shiiwz[.]pw
- s7610rir[.]pw
- privatlab[.]net
- privatlab[.]com
- 158[.]69[.]36[.]149
- 93[.]115[.]26[.]251
- 93[.]115[.]25[.]139
- 89[.]147[.]109[.]208
- 84[.]32[.]188[.]57
- 84[.]32[.]188[.]238
- 5[.]61[.]37[.]207
- 5[.]199[.]162[.]229
- 46[.]166[.]169[.]34
- 46[.]166[.]162[.]96
- 46[.]166[.]161[.]123
- 192[.]53[.]123[.]202

- 186[.]111[.]136[.]37
- 185[.]8[.]105[.]67
- 185[.]8[.]105[.]112
- 185[.]8[.]105[.]103
- 185[.]247[.]71[.]106
- 181[.]231[.]81[.]239
- 108[.]62[.]118[.]190

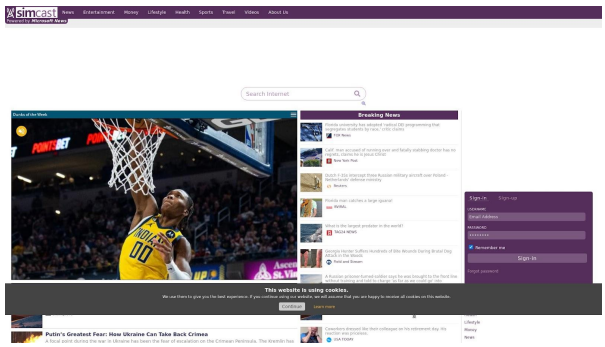
A bulk WHOIS lookup for the six domains showed they were managed by four registrars—REG.RU, LLC; Web4Africa Ltd.; PDR Ltd.; and GoDaddy.com, LLC. Three of them—s7610rir[.]pw, d6shiiwz[.]pw, and r77vh0[.]pw—also had unredacted registrant email addresses.

A bulk IP geolocation lookup for the IP addresses, meanwhile, revealed they were administered by nine Internet service providers (ISPs)—OVH Hosting; UAB Cherry Servers; 1984 ehf; LeaseWeb DE; Akamai Technologies, Inc.; Telecom Argentina S.A.; M247 Europe SRL; Telecom Argentina S.A.; and Leaseweb USA, Inc. spread across eight countries—Canada, Lithuania, Iceland, the Netherlands, Germany, Argentina, Sweden, and the U.S.

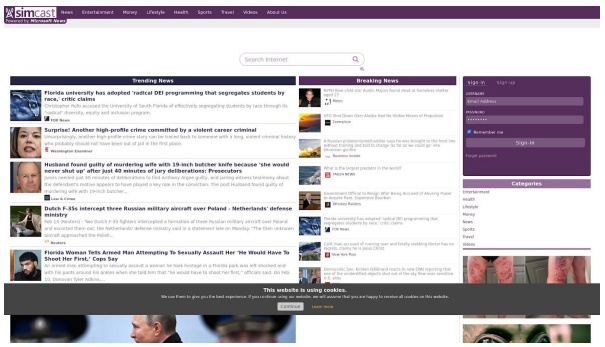


Using the domains identified as IoCs as DNS lookup terms led to the discovery of six IP addresses that aren't part of the Hive ransomware IoC list. Three of these are 172[.]217[.]20[.]206, 194[.]58[.]112[.]174, and 216[.]58[.]212[.]174. IP geolocation lookups for them showed that half were private hosts (hosting 5–15 domains each) while the remaining were shared (hosting at least 300 domains each).

After that, we used the IP addresses in the original IoC list and the additional ones we uncovered as reverse IP lookup terms. That gave us 936 additional domains, six of which were malicious. Two of them—11toon17[.]com and 85porn[.]cc—currently host or redirect to live content.



Screenshot of 11toon17[.]com



Screenshot of 85porn[.]cc

Our initial look at the domains tagged as IoCs also revealed a unique-looking string—***privatlab***. Scouring the DNS for other domains containing this string led to the discovery of 31 additional domains, one of which was malicious—laskyduniganprivatlab[.]com. And while the remaining domains containing the string ***privatlab*** weren't deemed malicious, the Hive ransomware group could easily commandeer and weaponize them for future attacks.

It's also interesting to note that some of the string-connected domains shared other similarities with those tagged as IoCs, such as their registrar (PDR Ltd. and REG.RU, LLC), creation year (2015), and registrant country (Iceland and the U.S.).

Screenshot lookups for the ***privatlab***-containing domains showed that 21 are unreachable, three are currently up for sale, and four are live. Among those that are accessible, one looks like a legitimate business website—privatlab[.]cc.

Screenshot of privatlab[.]cc

The purpose of the content hosted on the remaining three domains, however, was less clear. All three had the same content, one line that reads “A galaxy is made of stars.”

Screenshot of privatlab[.]ru, privatlab[.]su, and privatlab[.]eu

The Verdict

While the U.S. DOJ managed to decommission the Hive Ransomware Group's malicious infrastructure, it seems they've left some digital breadcrumbs that pointed to 970 yet-undisclosed web properties that could possibly be connected to the Hive ransomware via an IP host or unique string. Our IoC expansion analysis also led to the discovery of seven malware-hosting domains.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Domains That Shared the IoCs' IP Hosts

- 0-0-7[.]ru
- 0-100[.]online
- 0-22[.]ru
- 0-88[.]ru
- 0-ip[.]ru
- 0-iq[.]online
- 0-nds[.]ru
- 0-zaimo[.]ru
- 0000[.]network
- 0000[.]team
- 00001[.]ru
- 00008[.]ru
- 00010111[.]ru
- 000123[.]ru
- 000180[.]top
- 00049[.]online
- 00049[.]ru
- 000c[.]ru
- 000d[.]online
- 000d[.]ru
- 000e[.]ru
- 000p[.]online
- 000p[.]ru
- 000s[.]ru
- 000tiktok[.]com
- 000xs[.]net
- 000yahoo[.]com
- 0014[.]ru
- 0015[.]ru
- 00154021-836e-4c82-9fb4-fb4abf951347[.]pong[.]s[.]elliq[.]co
- 00174[.]ru
- 001cdaee-0a08-4779-987f-b6b612361079[.]pong[.]s[.]elliq[.]co
- 001digital[.]ru
- 001ed026-f0c8-427f-98b0-dd12c87c31d7[.]pong[.]s[.]elliq[.]co
- 001ed23f-19e8-45bf-bb0f-c50d78506449[.]pong[.]s[.]elliq[.]co
- 001hash[.]vip
- 001pax[.]online
- 001r[.]online
- 001r[.]ru
- 001shop[.]online
- 001shop[.]ru
- 001taxi[.]online
- 001taxi[.]ru
- 001wmr[.]online
- 001wmr[.]ru
- 002[.]ooo
- 002200[.]ru

- 002ab93d-9893-4d39-9b53-d6f56ac610f5[.]pong[.]s[.]elliq[.]co
- 002hash[.]com
- 003-1[.]online
- 003-1[.]ru
- 0030000[.]ru
- 00334365-37ef-465b-90b4-bab6b513f00c[.]pong[.]s[.]elliq[.]co
- 0035[.]ru
- 0036e1aa-5900-4d70-b379-f39002dfd7ff[.]pong[.]s[.]elliq[.]co
- 003707d1-8524-4d1a-a29b-007d4253ae4f[.]pong[.]s[.]elliq[.]co
- 003974ff-f3e8-4904-b2b1-4e3ae24afb4c[.]pong[.]s[.]elliq[.]co
- 003b9c93-1afd-43da-9fff-8d3f53115152[.]pong[.]s[.]elliq[.]co
- 003d756d-4b8f-435c-a797-a611578d24f3[.]pong[.]s[.]elliq[.]co
- 003hash[.]vip
- 00402f0d-5e36-4738-b505-d763a54807b0[.]pong[.]s[.]elliq[.]co
- 004be9ba-fd8c-41c1-a05a-b157df12976d[.]pong[.]s[.]elliq[.]co
- 004hash[.]com
- 004hash[.]vip
- 004oce[.]com
- 0055603[.]com
- 005b28d3-145b-4e5b-ab44-4144c8bd0349[.]pong[.]s[.]elliq[.]co
- 005fe4e0-290a-4104-808a-e31dc100dbb0[.]pong[.]s[.]elliq[.]co
- 005hash[.]com
- 005hash[.]vip
- 00630ed2-d420-4e92-b2f7-024168413b84[.]pong[.]s[.]elliq[.]co
- 0064f406-1ce3-4172-a833-3c9a389207cd[.]pong[.]s[.]elliq[.]co
- 0066ea00-76a3-48ee-bc42-05c7393435a2[.]pong[.]s[.]elliq[.]co
- 006hash[.]com
- 006hash[.]vip
- 007291d6-8ada-4ca4-a599-6982f1218079[.]pong[.]s[.]elliq[.]co
- 0072ecb8-6cad-49a0-802d-8231912dcefb[.]pong[.]s[.]elliq[.]co
- 007515[.]com
- 0079c291-35b1-4ff9-b2a5-b2942a14f11e[.]pong[.]s[.]elliq[.]co
- 007hash[.]vip
- 007smm[.]com
- 007v[.]ru
- 0085[.]ru
- 0088cbc6-a078-4111-915c-14a2d569143d[.]pong[.]s[.]elliq[.]co
- 008hash[.]vip
- 0090000[.]ru
- 009009[.]ru
- 009hash[.]vip
- 00a9aec3-3638-4be0-a935-06c59c684f95[.]pong[.]s[.]elliq[.]co
- 00b07373-adc3-4869-b12a-824d73d6c3b1[.]pong[.]s[.]elliq[.]co
- 00b750d7-e698-4a64-a543-77cde5796d4f[.]pong[.]s[.]elliq[.]co
- 00cd6aff-7bd3-4d1d-a0a8-d644e4be4b54[.]pong[.]s[.]elliq[.]co
- 00d[.]ru
- 00ea00a0-6023-41f2-8ee7-65ff9557410a[.]pong[.]s[.]elliq[.]co
- 00ead7f7-462b-40c2-91f4-f57852fb02f0[.]pong[.]s[.]elliq[.]co
- 00f0719d-e82c-43d3-a03b-0491e7ba8ef6[.]pong[.]s[.]elliq[.]co
- 00mmp[.]com
- 00oo[.]online
- 00oo[.]ru
- 00ps[.]ru

Sample Malicious IP-Connected Domains

- 0dt[.]ru
- 0rder2819[.]ru
- 1-1-mag[.]com

Sample Domains Containing the String *Privatlab*

- privatlab[.]tv
- privatlab[.]bz
- privatlab[.]in
- privatlab[.]de
- privatlab[.]ru
- privatlab[.]co
- privatlab[.]pw
- privatlab[.]me
- privatlab[.]ca
- privatlab[.]nl
- privatlab[.]hu
- privatlab[.]cc
- privatlab[.]mn
- privatlab[.]uk
- privatlab[.]su