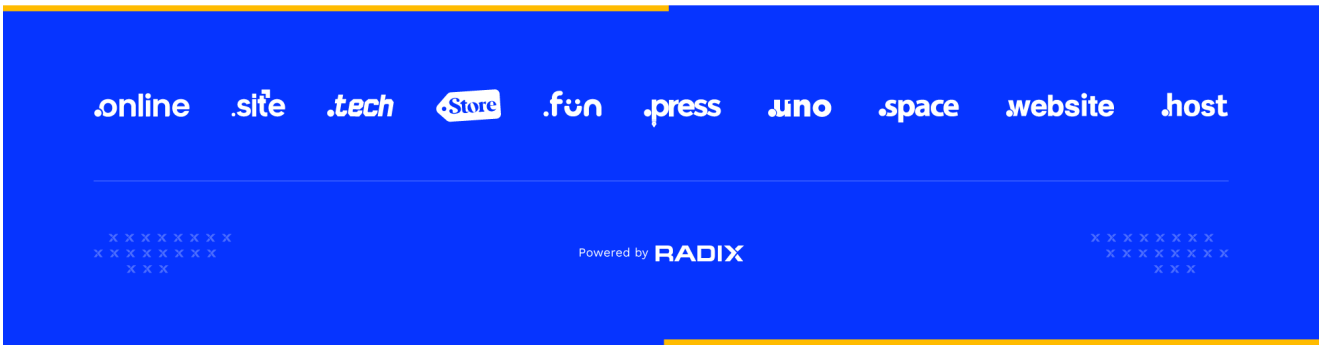
Signs of MuddyWater Developments Found in the DNS



By **WhoisXML API** (Sponsored Post) A Domain Research, Whois, DNS, and Threat Intelligence API and Data Provider

- August 24, 2023
- Views: 9,383

Cyber espionage group MuddyWater's or Mercury's first major campaign was seen as early as 2012. But as things always go in the cybersecurity realm, threat groups, especially those that gain infamy, don't necessarily just come and go.

Such is MuddyWater's case in that instead of disappearing, it resurfaces bigger and better each time. PhonyC2—the threat group's latest addition to its framework—is proof of that. Deep Instinct recently shone the spotlight on PhonyC2's underbelly by publishing an in-depth investigation on the matter.

WhoisXML API used the 27 IP addresses and 12 domains identified as PhonyC2 IoCs as jump-off points for a DNS deep dive, which led to the discovery of:

- Three additional unique IP addresses to which some of the domains identified as IoCs resolved
- Three domains that shared the dedicated IP hosts of the domains identified as IoCs
- 152 domains that contained strings found among the domains identified as IoCs
- 22 domains that contained the same strings as the IP-connected domains, two of which were classified as malicious by a bulk malware check

In addition, we analyzed the budding MuddyWater-DEV-1084 partnership that aimed to mask the former's involvement in targeted attacks to shed more light on recent ransomware campaigns. We specifically expanded a list of 14 IoCs published by Microsoft and uncovered:

- Three additional unique IP addresses to which some of the domains identified as IoCs resolved
- 294 domains that shared the dedicated hosts of the domains identified as IoCs, one of which turned out to be malicious based on a bulk malware check

A sample of the additional artifacts obtained from our analysis is available for download from our website.

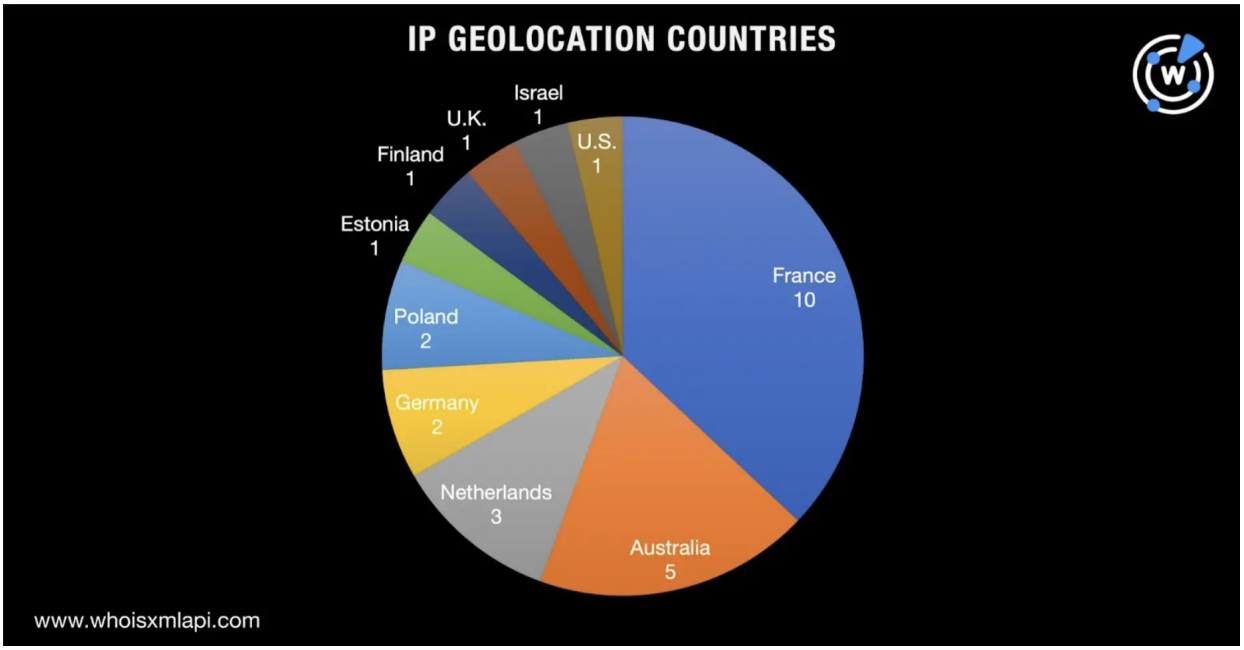
Part 1: PhonyC2 Traces Found in the DNS

What We Know about the PhonyC2 IoCs

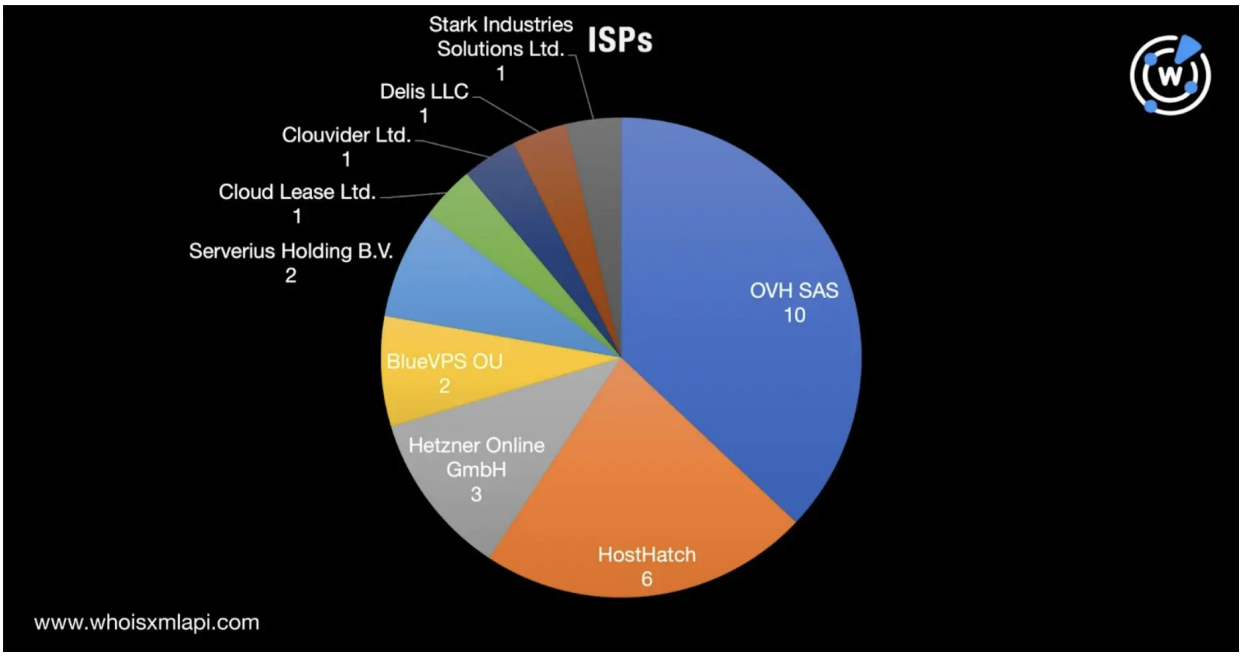
As mentioned above, Deep Instinct publicized 39 PhonyC2 IoCs, all part of the new MuddyWater C&C framework. We took a closer look at them using comprehensive DNS intelligence.

We subjected the IP addresses identified as IoCs to a bulk IP geolocation lookup and found that:

- France, Australia, and the Netherlands topped the list of geolocation countries, accounting for 10, five, and three IP addresses, respectively. The remaining nine IP addresses were scattered across seven other nations.



- OVH SAS, meanwhile, topped the list of ISPs, accounting for 10 of the IoCs. HostHatch and Hetzner Online GmbH completed the top 3, accounting for six and three IP addresses, respectively.



What We Learned about the PhonyC2 IoCs

We began our in-depth look at PhonyC2—the latest addition to the MuddyWater C&C framework—with Domains & Subdomains Discovery searches for strings found among the domains identified as IoCs, namely:

- **edc1.**
- **pru2.**
- **nno1.**
- **nno3.**
- **kwd1.**
- **kwd2.**
- **kwd3.**
- **qjk1.**
- **qjk2.**
- **qjk3.**
- **tes2.**
- **pru1.**

We uncovered 152 domains that started with the strings above. See how many we found for each in the table below.

STRING	VOLUME

edc1.	19
pru2.	10
nno1.	13
nno3.	9
kwd1.	11
kwd2.	7
kwd3.	14
qjk1.	11
qjk2.	13
qjk3.	14
tes2.	20
pru1.	11

While none of them were detected as malicious, some contained strings commonly found in web properties used or abused in nefarious campaigns, such as:

- **Adobe:** Seen in edc1[.]adobeaemcloud[.]com, which could figure in a cyber attack targeting the software developer or its product users.
- **ClouDNS:** Seen in edc1[.]cloudns[.]info, which couldn't be publicly attributed to ClouDNS and could be used in attacks trailing its sights on the DNS hosting service provider or its customers.
- **Yandex:** Seen in kwd3[.]storage[.]yandexcloud[.]net, which threat actors could utilize in malicious activities centered on the cloud platform or its users should it fall into the cracks and be forgotten by its owner.

Next, we subjected the 27 IP addresses identified as IoCs to reverse IP lookups. Three of them turned out to be dedicated hosts. In total, they hosted three domains that weren't part of the current IoC list—rare-upload[.]top, urbancritters[.]org[.]uk, and s2-store[.]com.

We searched for other domains containing the strings **rare-upload**, **urbancritters**, and **s2-store**. That allowed us to uncover 22 domains for two out of the three strings (**urbancritters**, and **s2-store**). Two of them turned out to be malicious based on a bulk malware check.

Both malicious domains were already unreachable at the time of writing. It was, however, interesting to note that one of them—refund-orderdc50kfcs2-store-apple[.]cf—alluded to Apple ownership. Its WHOIS record begged to differ, though. The malicious domain wasn't

publicly attributable to the tech giant.

Part 2: MuddyWater-DEV-1084 Partnership DNS Footprints

MuddyWater-DEV-1084 IoC Facts

Another recent MuddyWater-related development worthy of a closer look would be the group's collaboration with another threat group known as "DEV-1084."

In recent attacks believed to be spearheaded by MuddyWater, DEV-1084 took on the DarkBit persona to mask the former's involvement. Microsoft researchers, however, brought the partnership to light and publicized four domains and 10 IP addresses as IoCs.

MuddyWater-DEV-1084 IoC List Expansion Findings

To find artifacts connected to the MuddyWater-DEV-1084 attacks, we subjected the domains identified as IoCs to DNS lookups that revealed that three of them—pairing[.]rport[.]io, vatacloud[.]com, and ehorus[.]com—resolved to four unique IP addresses. While one of the resolving IP addresses was already identified as an IoC, the other three—49[.]12[.]228[.]207, 172[.]67[.]181[.]250, and 104[.]21[.]80[.]130—weren't.

Adding the three yet-unpublished IP hosts to those already identified as IoCs gave us a total of 13 IP addresses. Reverse IP lookups for them showed that three were dedicated hosts that were shared by 294 other domains, one of which—sdtvcs[.]ru—turned out to be a malware host.

A bulk WHOIS lookup result comparison, meanwhile, for the domains identified as IoCs and the 294 dedicated IP-connected domains revealed that:

- 36 of the IP-connected domains shared rport[.]io's registrar, four others shared that of ehorus[.]com, and 50 shared that of vatacloud[.]com
- 18 of the IP-connected domains shared rport[.]io's creation year, seven others shared that of ehorus[.]com, and 60 shared that of vatacloud[.]com
- 105 of the IP-connected domains shared rport[.]io's registrant country, one shared that of ehorus[.]com, and 44 shared that of vatacloud[.]com

---

Our MuddyWater investigation allowed us to identify 477 closely connected web properties that could be considered PhonyC2 and Mercury-DEV-1084 attack artifacts. It also led to the discovery of three malicious domains worth taking note of.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be

deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.

By **WhoisXML API, A Domain Research, Whois, DNS, and Threat Intelligence API and Data Provider**

Whois API, Inc. (WhoisXML API) is a big data and API company that provides domain research & monitoring, Whois, DNS, IP, and threat intelligence API, data and tools to a variety of industries.

Visit Page

Filed Under

Comments

Commenting is not available in this channel entry.
CircleID Newsletter The Weekly Wrap
More and more professionals are choosing to publish critical posts on CircleID from all corners of the Internet industry. If you find it hard to keep up daily, consider subscribing to our weekly digest. We will provide you a convenient summary report once a week sent directly to your inbox. It's a quick and easy read.

> I make a point of reading CircleID. There is no getting around the utility of knowing what thoughtful people are thinking and saying about our industry.

Related