Nozomi Networks Researchers Track Malicious Glupteba Activity Through the Blockchain

nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain/

by Nozomi Networks Labs December 15, 2022

Threat actors are increasingly leveraging blockchain technology to launch cyberattacks. By taking advantage of the distributed and decentralized nature of blockchain, malicious actors can exploit its anonymity for a variety of attacks, ranging from malware propagation to ransomware distribution.

The Glupteba trojan is an example of a threat actor leveraging blockchain-based technologies to carry out their malicious activity. In this blog, Nozomi Networks Lab presents our latest findings on Glupteba and how security teams can search for malicious activity in the blockchain.

Nozomi Networks Researchers have tracked Glupteba through the blockchain, identifying 15 Glupteba bitcoin addresses spawning over four years, through four different campaigns.

What is Glupteba?

Glupteba is a backdoor trojan that is downloaded via Pay-Per-Install networks – online ad campaigns that prompt software or application downloads – in infected installers or software cracks. Once Glupteba is active on a system, the botnet operators can deploy additional modules from the credential stealer to exploit kits compromising devices on the target network. There are several Glupteba modules aimed at exploiting vulnerabilities in various Internet of Things (IoT) appliances from vendors, such as MikroTik and Netgear.

Surprisingly, Glupteba leverages the Bitcoin blockchain to distribute its Command and Control (C2) domains to infected systems. Apart from the fact that this is an uncommon technique, this mechanism is also extremely resilient to takedowns as there is no way to erase nor censor a validated Bitcoin transaction. Using the same approach that Glupteba is using to hide data within the blockchain, researchers can hunt for malicious transactions and recover their payloads. If the said domains are not stored in plaintext, reversing the Glupteba samples enables security researchers to decrypt the payload and access the embedded domains.

Using the Blockchain to Store Data

The Bitcoin blockchain can be used to store arbitrary data. This is made possible by the `OP_RETURN` opcode that enables storage of up to 80 bytes of arbitrary data within the signature script. This storage mechanism has several advantages. First, it is resilient to takedowns. Once a transaction has been validated, there is no way to erase it – this is the nature of the blockchain. Using this mechanism to distribute C2 domain means that law enforcement officers, network defenders, and incident responders have no way to take down the Bitcoin address and erase the transaction. The way the Bitcoin blockchain is built on top of modern cryptography also makes this mechanism secure; without the Bitcoin address private key, one cannot send a transaction with such a data payload originating from the malicious address, hence, taking over the botnet is not possible. Additionally, threat actors can encrypt their payload from peering eyes, making the data storage scheme robust and cost effective.

This technique has also been used by the Cerber ransomware in the past. Bitcoin transactions originating from specific addresses were monitored and the first 6 characters of a destination address were used along with a `.top` TLD appended to> generate a domain, which would be used to query the active C2 infrastructure.

Glupteba is known to be using a similar mechanism relying on `OP_RETURN` instead of destination addresses to distribute its C2 domains. In case of a C2 domain being taken down, the botnet operators only need to send a new transaction from the Bitcoin address distributing the domains and voila, the malware will adjust its configuration the next time the C2 is refreshed. The latest identified Glupteba bitcoin transaction dates to the 8th of November 2022 with its embedded payload `000c0b0006171c11064d150a0b16`.

The hexadecimal payload above does not seem to represent anything close to a domain name and that is because Glupteba uses, in its latest variant, a XOR encryption scheme to protect the data. Once the key is known, typically by reverse engineering a sample such as c6d4ce67dd25764f571a84caa19fa6c2b067cae6, decrypting the data becomes simple; see a sample of this decryption in Github.

The Evolution of Glupteba

Glupteba is known to use the Bitcoin blockchain to distribute its C2 servers since at least 2019. To retrieve the Bitcoin transactions, several providers are used, usually *blockchain.com* and *blockstream.info*. The Glupteba function responsible for querying *blockchain.com* to retrieve the transaction data is shown in Figure 1.

```
int __usercall main_discoverDomain_func2@<eax>()
{
  int v1; // [esp+Ch] [ebp-18h]
  int v2[2]; // [esp+1Ch] [ebp-8h] BYREF

  v2[0] = (int)&unk_6E5800;
  v2[1] = (int)&off_7D6600;
  v1 = log_Println(v2, 1, 1);
  application_resilience_blockchaincom_DiscoverDomain(
    (int)off_C47AAC,
    (int)"1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD9735527136788
    34);
  return v1;
}
```

Figure 1.

The Bitcoin address that contains the transactions with the command-and-control domains.

The way the domains are protected within the transactions has slightly evolved over time. In 2019, Glupteba used AES-GCM to protect and embed the data in the bitcoin transactions. Each sample was shipped with a hardcoded key and initialization vector enabling the sample to decrypt the payload from the Bitcoin transaction. Figure 2 shows the decryption routine in the oldest Glupteba versions. .

```
result = a2;
if ( a2 > 0 )
{
  for ( i = 0; ; i = v15 + 1 )
  {
    v18 = a1;
    v15 = i;
    OpReturnData = application_resilience_blockchaincom_getOpReturnData(*a1, a1[1], a1[2], a4, a5, v9, v10, v11);
    if ( v10 )
    {
      v17 = v9;
      v8 = ((__int64 (*)(void))loc_451230)();
      v15 = application_aes256gcm_Decrypt(v16, 32, 32, v17, v8, HIDWORD(v8), v10, v11, OpReturnData, v13, v14);
      result = v10;
      if ( !v13 )
        break;
    }
    result = v15 + 1;
    if ( v15 + 1 >= a2 )
      break;
    a1 = v18 + 3;
  }
}
return result;
}
```

Figure 2.

The Glupteba code calling the AES-GCM decryption routine.

In newer versions of the malware, this scheme was switched to a simple XOR cipher, which is currently being used. All samples we found were using the same key: “cheesesauce”. Figure 3 shows this key being moved around in memory in the function responsible to decrypt the ciphertext.

```
int __usercall application_xor_EncryptDecrypt@<eax>(_BYTE *a1, int a2, int a3, int a4, unsigned int a5)
{
  _BYTE *v5; // eax
  int v6; // ecx
  int result; // eax
  signed int v8; // edx
  int v9; // ebx
  signed int v10; // esi
  char v11; // al
  int v12; // edi
  char v13; // di
  unsigned int v14; // ebx
  unsigned int i; // edx
  int v16; // [esp+0h] [ebp-20h]
  int v17; // [esp+4h] [ebp-1Ch]
  _BYTE v18[11]; // [esp+11h] [ebp-Fh] BYREF
  int v19; // [esp+1Ch] [ebp-4h]
  _BYTE *key; // [esp+24h] [ebp+4h]
  int v21; // [esp+28h] [ebp+8h]

  if ( a2 )
  {
    v5 = a1;
    v6 = a2;
  }
  else
  {
    qmemcpy(v18, "cheesesauce", sizeof(v18));
```

Figure 3. The XOR cipher key is being loaded in the Glupteba decryption routine.

Timeline of Events

Given all that information, we went on a blockchain harvesting tour, scanning the entire Bitcoin blockchain for hidden C2 domains. We tried to decrypt the data payload of the `OP_RETURN` script present in each transaction of every block using all the algorithms and keys we know to be associated with Glupteba. In addition, we downloaded over 1500 Glupteba samples from VirusTotal and looked at the wallet addresses they used to make sure we did not miss anything. But that is not all: the latest set of TLS certificates Glupteba uses also exhibits a precise pattern in the Subject Alternative Names and, thanks to certificate transparency, this can be hunted for. Finally, we also took a close look at the passive DNS records at our disposal to find potential associated domains and hosts.

This research gave us a massive series of events we decided to summarize with the timeline below, showing when actions were taken by Glupteba operators.

Date	Source	Description
2022-11-22	Passive DNS	Domain registration limeprime[.]org
2022-11-21	Passive DNS	Domain registration greenphoenix[.]xyz
2022-11-08	Blockchain	Wallet 1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK update cdneurops[.]pics

Date	Source	Description
2022-10-29	Blockchain	• Wallet 1NX7zTP6C4oGj2y3DaJTrg26AGFWExvYnr update mastiakele[.]icu • Wallet 1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd update mastiakele[.]xyz • Wallet 1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK update cdneurops[.]buzz • Wallet 1CfevVPC8cSpFf7QKQwShrFgQYfyQaoXhc update cdneurops[.]shop • Wallet 14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs update zaoshanghaoz[.]net • Wallet 1BrEshrz6gVbVuHGBgJ5GuHBvC2sdoeTAJ update cdneurop[.]cloud • Wallet 1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK update cdneurop[.]cloud • Wallet 1AuWUMtjPo7Cc1Ji2pz7DWVvVJ5EjiUaHh update cdneurops[.]health • Wallet 1BqY56No1LR64AGcog4mF54UTPnjrPAPHz update mastiakele[.]cyou • Wallet 1CfevVPC8cSpFf7QKQwShrFgQYfyQaoXhc update mastiakele[.]cyou • Wallet 14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs update zaoshanghaoz[.]net • Wallet 1NX7zTP6C4oGj2y3DaJTrg26AGFWExvYnr update mastiakele[.]icu • Wallet 1Mz2b2onxnAYhJTJQoGHdSBy6wu2HpufVR update mastiakele[.]ae[.]org • Wallet 1MuJwQKLQKt1VCBQ9u1RtepW7sDD3AwRE6 update zaoshang[.]ooo • Wallet 19RzEN3pqHvgRHGMjjtYCqjVTXt8bnHkK3 update cdntokiog[.]studio • Wallet 1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd update cdntokiog[.]studio • Wallet 1HSC8Yt2yjuFUSGpUfJnwLMr4HzNxV3dvP` update zaoshang[.]moscow • Wallet 15nWGFaodg3efVKATgsaaSPU2TxSbiMHcP update окрф[.]рф • Wallet 1LQ2EPBwPqdbmXwN6RodPS4xqcm8EtPcaB update zaoshang[.]ru • Wallet 1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN update zaoshanghao[.]su
2022-10-28	Certificate Transparency	Let’s encrypt certificate registration
2022-10-28	Blockchain	Wallet 1BL6NZSoXtMSdquRmePDUCQxFaXtLLSVWG update duniadekho[.]bar

Date	Source	Description
2022-10-27	Passive DNS	Domain registration cdneurops[.]pics mastiakele[.]icu mastiakele[.]xyz cdneurops[.]buzz cdneurops[.]shop zaoshanghaoz[.]net cdneurop[.]cloud cdneurops[.]health mastiakele[.]cyou mastiakele[.]ae[.]org zaoshang[.]ooo cdntokiog[.]studio zaoshang[.]moscow окрф[.]рф zaoshang[.]ru zaoshanghao[.]su duniadekho[.]bar
2022-10-26	Blockchain	Wallet 1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK update checkpos[.]net
2022-10-25	Passive DNS	Domain registration checkpos[.]net
2022-10-01	Passive DNS	Domain registration revouninstaller[.]homes
2022-09-30	Blockchain	Wallet 1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN update tmetres[.]com
2022-09-28	Passive DNS	Domain registration tmetres[.]com
2022-08-12	Blockchain	• Wallet 1BL6NZSoXtMSdquRmePDUCQxFaXtLLSVWG update 3ebu257qh2dlauxqj7cgv3i55e4orb55mwgqf4tq7eicsa3dfhr4aaid[.]onion • Wallet 1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN update yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad[.]onion
2022-08-12	Passive DNS	Domain registration getyourgift[.]life
2022-07-04	Blockchain	• Wallet 1Cxy9e6KtHtBJrQwCwpKgcyp6dhncx6eNh update x4l2doee6uhhf3lqjvjodgqtxsjvwbkdqyldhwyhwkhf4y23aqq7jayd[.]onion • Wallet 1HSC8Yt2yjuFUSGpUfJnwLMr4HzNxV3dvP update bihgkrr546ctjdn4mwr7x4bhvwz55sftx6xir6cwlfo6rhppd2eu7syd[.]onion
2022-06-09	Blockchain	Wallet 1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd update x4l2doee6uhhf3lqjvjodgqtxsjvwbkdqyldhwyhwkhf4y23aqq7jayd.onion
2022-06-07	Blockchain	Wallet 1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd update x4l2doee6uhhf3lqjvjodgqtxsjvwbkdqyldhwyhwkhf4y23aqq7jayd.onion

Date	Source	Description
2022-06-06	Blockchain	• Wallet 1AuWUMtjPo7Cc1Ji2pz7DWVvVJ5EjiUaHh update c43tnmrkzfmkjyd3j4v6xbyrd67q6pskzy67dwkzj36uoqwpoju2loyd.onion • Wallet 1CfevVPC8cSpFf7QKQwShrFgQYfyQaoXhc update 2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad.onion • Wallet 1BrEshrz6gVbVuHGBgJ5GuHBvC2sdoeTAJ update yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad.onion • Wallet 19RzEN3pqHvgRHGMjjtYCqjVTXt8bnHkK3 update dg2sz7pxs7llf2t25fsbutlvvrjij4pmojugn75cmxnvoshmju6dzcad.onion • Wallet 1HSC8Yt2yjuFUSGpUfJnwLMr4HzNxV3dvP update c43tnmrkzfmkjyd3j4v6xbyrd67q6pskzy67dwkzj36uoqwpoju2loyd.onion • Wallet 1BqY56No1LR64AGcog4mF54UTPnjrPAPHz update 2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad.onion • Wallet 1LQ2EPBwPqdbmXwN6RodPS4xqcm8EtPcaB update dg2sz7pxs7llf2t25fsbutlvvrjij4pmojugn75cmxnvoshmju6dzcad.onion • Wallet 15nWGFaodg3efVKATgsaaSPU2TxSbiMHcP update papmcl4r32awafck75y5446n252qqqq4h6c4y2slaayposrtfbcebdqd.onion • Wallet 14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs update c43tnmrkzfmkjyd3j4v6xbyrd67q6pskzy67dwkzj36uoqwpoju2loyd.onion
2022-06-03	Blockchain	• Wallet 1Mz2b2onxnAYhJTJQoGHdSBy6wu2HpufVR update 2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad.onion • Wallet update 1MuJwQKLQKt1VCBQ9u1RtepW7sDD3AwRE6 dg2sz7pxs7llf2t25fsbutlvvrjij4pmojugn75cmxnvoshmju6dzcad.onion • Wallet update 14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs papmcl4r32awafck75y5446n252qqqq4h6c4y2slaayposrtfbcebdqd.onion • Wallet update 1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad.onio • Wallet 1Cxy9e6KtHtBJrQwCwpKgcyp6dhncx6eNh update yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad.onio
2022-06-01	Blockchain	• Wallet 1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK update dg2sz7pxs7llf2t25fsbutlvvrjij4pmojugn75cmxnvoshmju6dzcad.onion • Wallet 1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd update maesvpovrwqfaqjw44bbeb2w62h6n7eyosbeit7rfrrdbyjymqaxfryd.onion
2021-12-29	Blockchain	Wallet 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 update dafflash[.]com
2021-12-27	Blockchain	Domain registration dafflash[.]com
2021-12-25	Blockchain	Wallet 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 update filimaik[.]com
2021-12-13	Blockchain	Wallet 12EfzLra6LttQ8RWvBTDzJUjYE6eRxx4TY update 7owe32rodnp3vnx2ekqncoegxolkmb3m2fex5zu6i2bg7ktivhwvczqd.onion
2021-12-12	Blockchain	Wallet 12EfzLra6LttQ8RWvBTDzJUjYE6eRxx4TY update r5vg4h5rlwmo6oa3p3vlckuvf5na2wb2tnqbsbkivhrhlyze6czlpjad.onion

Date	Source	Description
2021-12-10	Passive DNS	Domain registration godespra[.]com filimaik[.]com
2021-12-09	Blockchain	Wallet 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 update mydomelem.com
2021-12-08	Blockchain	Wallet 1HjoomvzjtvZdbznoEijTNAkMjmsFba9fY update nameiusr.com
2021-12-07	Blockchain	Wallet 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 update younghil.com
2021-12-06	Passive DNS	Domain registration mydomelem.com nameiusr.com younghil.com
2021-11-09	Blockchain	Wallet 1GLjCyG3fDf7vT3SxwtEUx7Z2w2UQrR3FU update newcc[.]com
2021-10-19	Blockchain	Wallet 1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1 update nisdably[.]com
2021-10-13	Blockchain	Wallet 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 update tyturu[.]com
2021-10-11	Passive DNS	Domain registration tyturu[.]com
2021-03-28	Passive DNS	Domain registration nisdably[.]com
2020-05-13	Blockchain	Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update maxbook[.]space
2020-05-07	Blockchain	Wallet 1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1 update easywbdesign[.]com
2020-04-08	Blockchain	Wallet 1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1 update sndvoices[.]com
2020-04-02	Passive DNS	Domain registration easywbdesign[.]com sndvoices[.]com
2020-03-28	Blockchain	• Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update myinfoart[.]xyz • Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update gfixprice[.]xyz • Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update getfixed[.]xyz
2020-03-15	Passive DNS	Domain registration maxbook[.]space

Date	Source	Description
2020-02-17	Blockchain	Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update anotheronedom[.]com
2020-02-17	Passive DNS	Domain Registration anotheronedom[.]com
2020-02-14	Blockchain	Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update sleepingcontrol[.]com
2020-01-24	Blockchain	Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update robotatten[.]com
2020-01-23	Blockchain	Wallet 34RqywhujsHGVPNMedvGawFufFW9wWtbXC update robotatten[.]com
2020-01-23	Passive DNS	Domain registration sleepingcontrol[.]com robotatten[.]com
2019-06-19	Blockchain	Wallet 15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 update venoxcontrol[.]com
2019-06-14	Passive DNS	Domain registration venoxcontrol[.]com

The 4 Glupteba Campaigns

We have been able to identify 15 Glupteba bitcoin addresses spawning over 4 years and what we believe to be 4 different campaigns.

Campaign 1

The oldest wave seems to have started in June 2019. Back then, only one single Bitcoin address was used to distribute the malicious domains. This also corroborates what Google found out in their lawsuit against two Glupteba operators.

Address	First seen	Last seen	Transactions	Number of samples
15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6	2019-06-17 15:51	2020-05-13 13:02	16	54

Figure 4 shows a graph of the address transactions. We can see the `OP_RETURN` transactions like 3Jt2U where the funds bounce back to the 15y7d address. Interestingly all the remaining $36.18 on the 15y7d address were sent to the address 3Jwj7 in February 2020. No activity has been observed at that address since then.

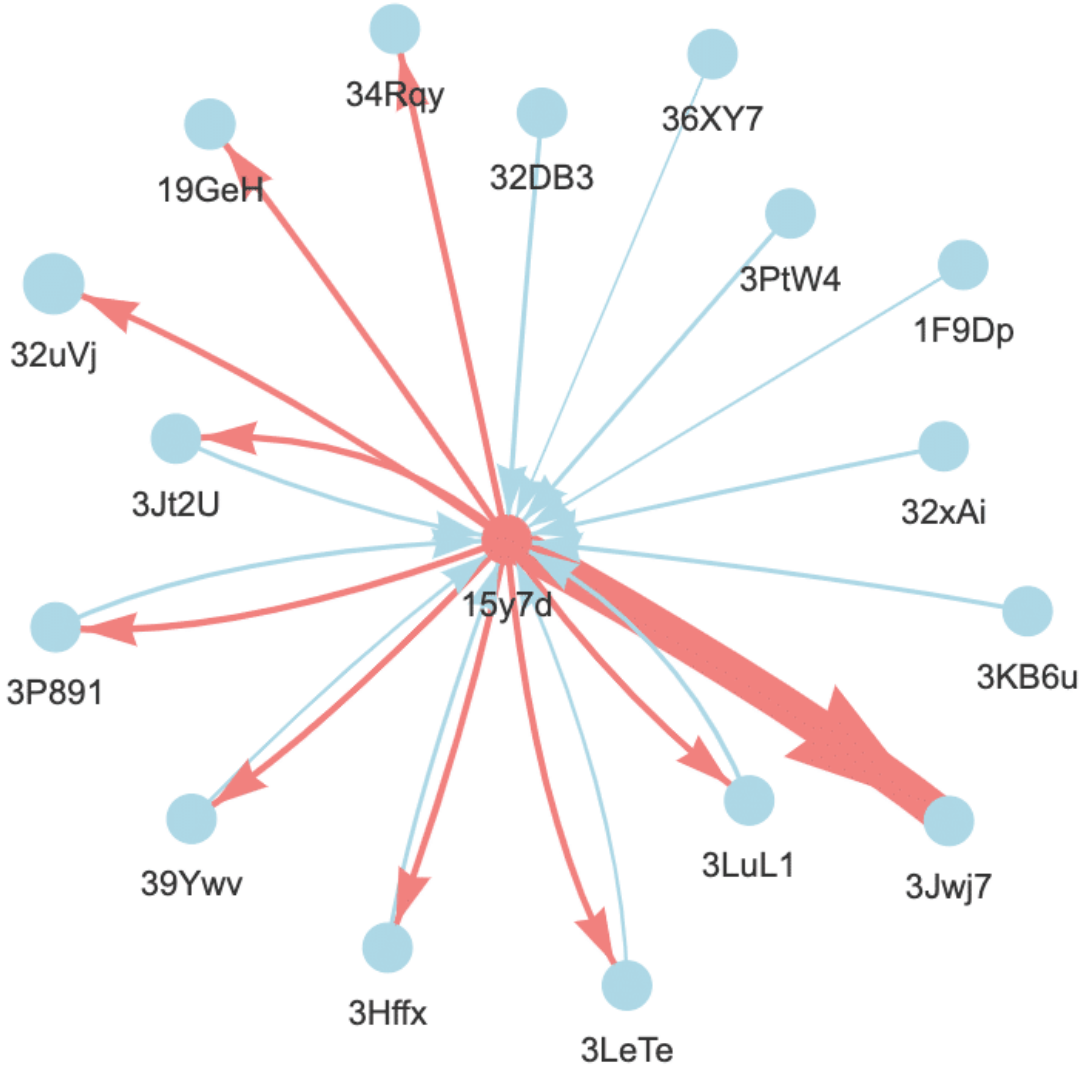

Figure 4.

The graph shows the transaction to and from the address involved in the 2019 campaign.

Campaign 2

The second wave seems to have started in April 2020, this time two Bitcoin addresses were used to distribute the malicious C2 domains. Interestingly we did not find any samples using the second address; it could be a testing address to ensure the Glupteba variants were behaving as expected. In addition, the domain distributed via the supposedly testing address *deepsound[.]live* has not been seen in any other transactions we were able to find across both addresses. It could also be that we simply are missing some samples.

Address	First Seen	Last seen	Transactions	Number of samples
1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1	2020-04-08 18:28	2021-10-19 17:28	11	87

Address	First Seen	Last seen	Transactions	Number of samples
1bRfcRZVws98j3QQEZxrgRVd15vVF6zSU	2020-04-08 14:21	2020-04-08 15:49	2	0

Here the same pattern can be observed on the main address 1CgPC, after a period of activity, the remaining funds accounting for $28.45 were transferred back to some vendor or merchant in November 2021. At the supposed test Bitcoin address, the funds were not transferred and remain to this day on the account for a balance of $76.80. Figure 5 shows the transactions to and from both addresses.

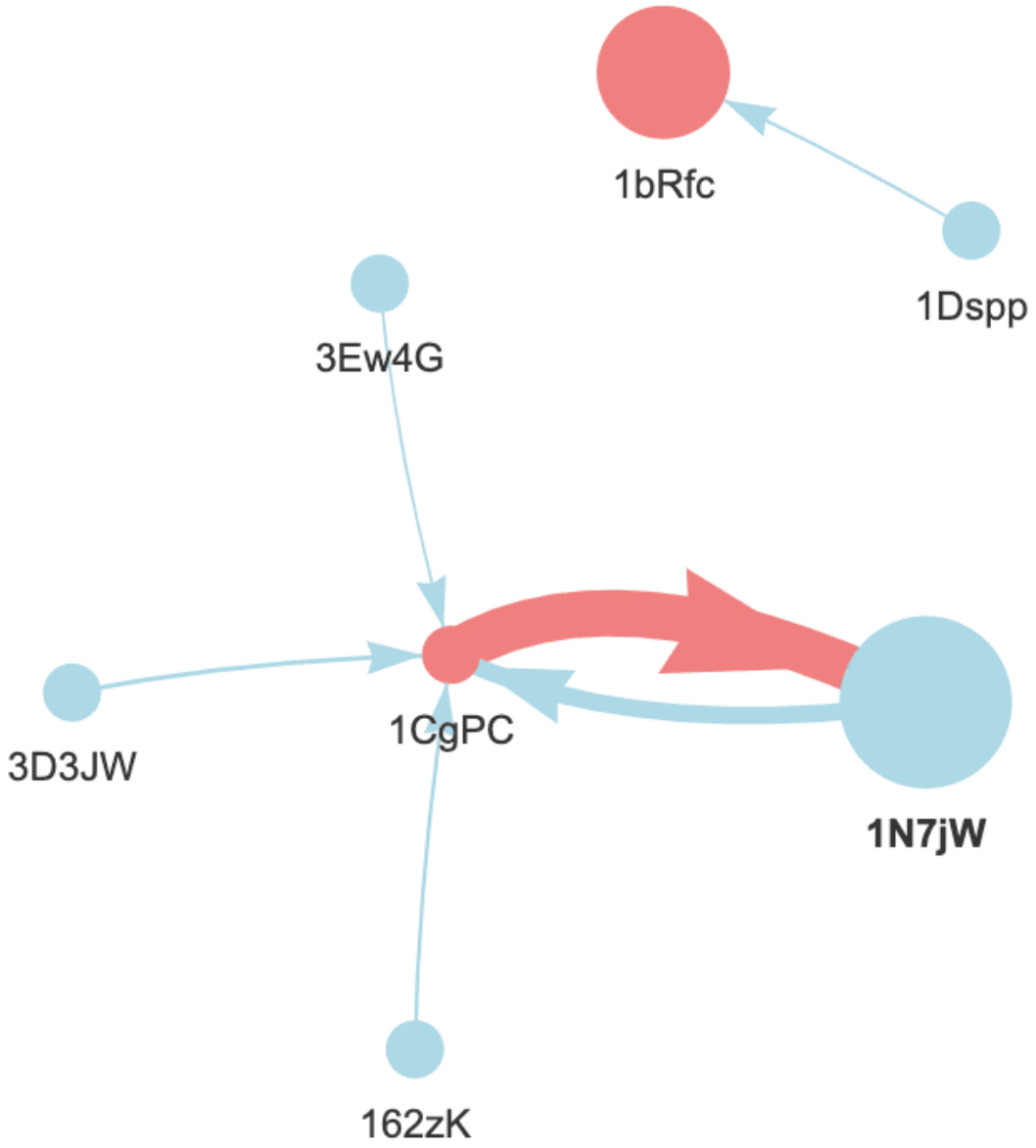

Figure 5.

The graph shows the transaction to and from the addresses involved in the 2020 Glupteba

campaign.

Campaign 3

The third campaign starts in November 2021; the number of bitcoin addresses used to deliver malicious domain doubled, from 2 in 2020 to 4 in 2021. This campaign was the shortest of all, with a lifespan of only about two months. We believe this is likely due to Google efforts to take the botnet down, when about a~~1~~ year ago Google filed a lawsuit against Glupteba two operators and several actions were taken to disrupt the botnet operations. This is also the first time TOR hidden services were used as a command-and-control server by Glupteba.

Address	First seen	Last seen	Transactions	Number of samples
1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97	2021-10-13 15:20	2021-12-29 10:15	12	77
12EfzLra6LttQ8RWvBTDzJUjYE6eRxx4TY	2021-12-12 21:38	2021-12-13 21:14	3	3
1HjoomvzjtvZdbznoEijTNAkMjmsFba9fY	2021-12-08 15:57	2021-12-08 17:12	2	17
1GLjCyG3fDf7vT3SxwtEUx7Z2w2UQrR3FU	2021-11-09 12:22	2021-11-09 12:49	2	0

Glupteba operators used four wallets, with the most active one being 1CUha as shown in Figure 6. Again, there were no remaining funds left on the Bitcoin addresses. This is also the oldest address in this campaign and the one with the highest number of transactions. Interestingly, we were not able to find a single sample referring to the address 1GLjC which we believe could have been used for testing the malware, similar to 2020. The domain used *newcc[.]*com was also not registered at the time and could indicate it was used in a testing environment or we could be missing some samples.

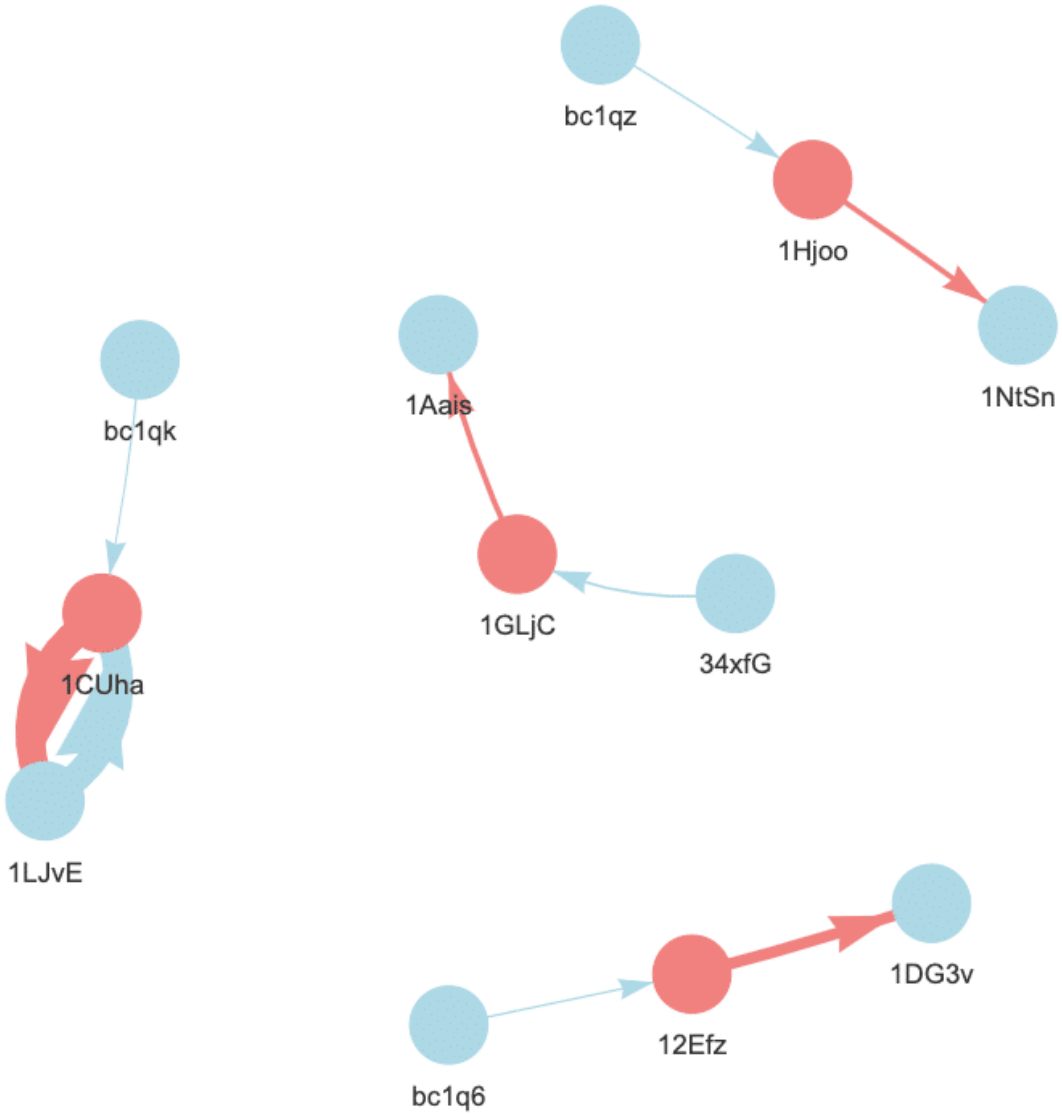

Figure 6.

The graph shows the transaction to and from the addresses involved in the 2021 Glupteba campaign.

Campaign 4

The latest and ongoing campaign started in June 2022, 6 months after the Google lawsuit, and this time the number of malicious bitcoin addresses significantly increased. We believe this is due to several factors. First, having more Bitcoin addresses makes security researcher job more complicated. Second, to show that the Google lawsuit did not have a major effect on their Glupteba operations. For this campaign we were not able to find any samples for 3 of the addresses we gathered. We believe these addresses are not made for testing as they distribute some domains found in other Bitcoin addresses for which we found samples. In addition, there was a tenfold increase in TOR hidden service being used as C2 servers since the 2021 campaign.

Address	First seen	Last seen	Transactions	Number of samples
1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK	2022-06-01 14:16	2022-11-08 11:54	11	1197
1LQ2EPBwPqdbmXwN6RodPS4xqcm8EtPcaB	2022-06-03 13:59	2022-10-29 11:29	4	6
1MuJwQKLQKt1VCBQ9u1RtepW7sDD3AwRE6	2022-06-03 15:02	2022-10-29 11:37	4	6
1Mz2b2onxnAYhJTJQoGHdSBy6wu2HpufVR	2022-06-03 14:33	2022-10-29 11:40	5	3
1NX7zTP6C4oGj2y3DaJTrg26AGFWExvYnr	2022-06-06 14:10	2022-10-29 12:07	6	6
14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs	2022-06-03 14:56	2022-10-29 12:03	8	12
15nWGFaodg3efVKATgsaaSPU2TxSbiMHcP	2022-06-03 14:34	2022-10-29 11:30	6	48
19RzEN3pqHvgRHGMjjtYCqjVTXt8bnHkK3	2022-06-06 13:51	2022-10-29 11:37	4	6
1AuWUMtjPo7Cc1Ji2pz7DWVvVJ5EjiUaHh	2022-06-06 14:04	2022-10-29 11:43	4	3
1BL6NZSoXtMSdquRmePDUCQxFaXtLLSVWG	2022-06-07 08:51	2022-10-28 10:51	4	3
1BqY56No1LR64AGcog4mF54UTPnjrPAPHz	2022-06-04 07:59	2022-10-29 11:41	4	3
1BrEshrz6gVbVuHGBgJ5GuHBvC2sdoeTAJ	2022-06-04 02:35	2022-10-29 11:42	4	3

Address	First seen	Last seen	Transactions	Number of samples
1CfevVPC8cSpFf7QKQwShrFgQYfyQaoXhc	2022-06-06 14:05	2022-10-29 12:10	6	3
1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN	2022-06-03 13:55	2022-10-29 11:28	8	3
1HSC8Yt2yjuFUSGpUfJnwLMr4HzNxV3dvP	2022-06-06 13:58	2022-10-29 11:33	6	0
1Cxy9e6KtHtBJrQwCwpKgcyp6dhncx6eNh	2022-06-03 14:05	2022-07-04 16:07	4	0
1CzetoTU29WbhNy1UozrQpxuFuCVxffbTd	2022-05-31 15:19	2022-10-29 12:04	8	0

The transactions graphs shown in Figure 7 involving the addresses used in the 2022 campaign show the upscaling of the operations since 2019. Lastly, we traced back these transactions even further, and we believe that at least five different merchants and exchanges were used to fund the Glupteba addresses since 2019.

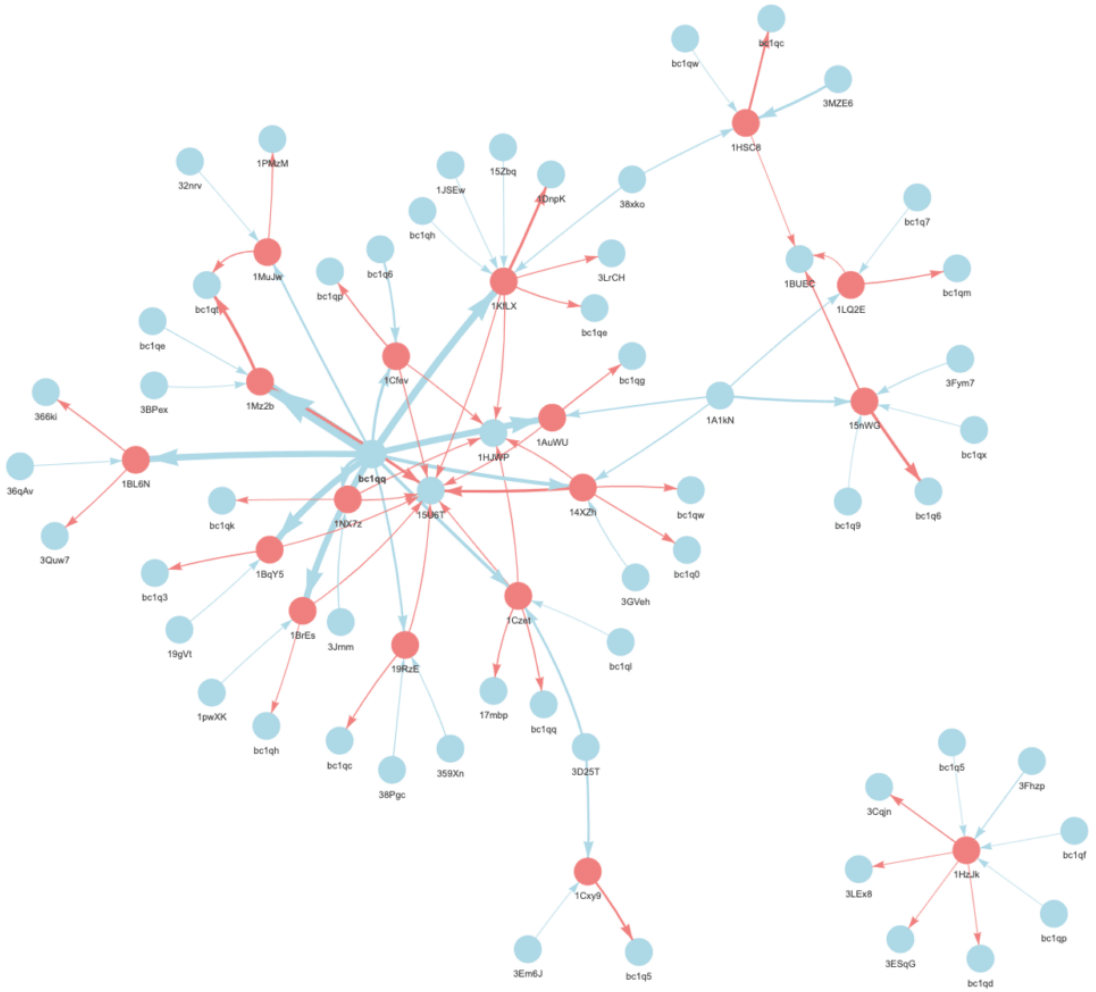

Figure 7.

The graph shows the transaction to and from the addresses involved in the 2022 campaign.

Conclusion

In this blog, we have shown how Glupteba can be hunted by following blockchain transaction, TLS certificate registrations, and by reverse engineering samples. We also had a look at how the blockchain can be used to store arbitrary data and how threat actors leverage this in the wild. In addition, we tried to shed some light on the Glupteba campaigns over the years. In terms of resilience, we have seen how the actions Google took to disrupt the Glupteba botnet had an impact on the 2021 campaign, which we believe ended abruptly. Even with Google winning a favorable ruling recently, we hoped it would have inflicted a severe blow to Glupteba operations, but almost a year later we can say it most likely did not. Indeed, it took Glupteba about six months to build a new campaign from scratch and distribute it in the wild, and this time on a much larger scale.

For defenders and responders, we strongly suggest blocking blockchain-related domains like blockchain.info but also Glupteba known C2 domains in your environment. We also recommend monitoring DNS logs and keeping the antivirus software up to date to help prevent a potential Glupteba infection.

Indicators of Compromise

IOC	Description
cdneurops[.]pics	C2 domain 2022
mastiakele[.]icu	C2 domain 2022
mastiakele[.]xyz	C2 domain 2022
cdneurops[.]buzz	C2 domain 2022
cdneurops[.]shop	C2 domain 2022
zaoshanghaoz[.]net	C2 domain 2022
cdneurop[.]cloud	C2 domain 2022
cdneurops[.]health	C2 domain 2022
mastiakele[.]cyou	C2 domain 2022
zaoshanghaoz[.]net	C2 domain 2022
mastiakele[.]ae[.]org	C2 domain 2022
zaoshang[.]ooo	C2 domain 2022
cdntokiog[.]studio	C2 domain 2022
zaoshang[.]moscow	C2 domain 2022
zaoshang[.]ru	C2 domain 2022
zaoshanghao[.]su	C2 domain 2022
duniadekho[.]bar	C2 domain 2022
checkpos[.]net	C2 domain 2022
dafflash[.]com	C2 domain 2021
godespra[.]com	C2 domain 2021
filimaik[.]com	C2 domain 2021
mydomelem[.]com	C2 domain 2021
nameiusr[.]com	C2 domain 2021
younghil[.]com	C2 domain 2021

IOC	Description
newcc[.]com	C2 domain 2021 (potential testing domain)
nisdably[.]com	C2 domain 2021
tyturu[.]com	C2 domain 2021
maxbook[.]space	C2 domain 2020
easywbdesign[.]com	C2 domain 2020
sndvoices[.]com	C2 domain 2020
myinfoart[.]xyz	C2 domain 2020
gfixprice[.]xyz	C2 domain 2020
getfixed[.]xyz	C2 domain 2020
anotheronedom[.]com	C2 domain 2020
sleepingcontrol[.]com	C2 domain 2020
robotatten[.]com	C2 domain 2020
deepsound[.]live	C2 domain 2020 (potential testing domain)
venoxcontrol[.]com	C2 domain 2019
3ebu257qh2dlauxqj7cgv3i55e4orb55mwgqf4tq7eicsa3dfhr4aaid[.]onion	C2 domain 2022
yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad[.]onion	C2 domain 2022
x4l2doee6uhhf3lqjvjodgqtxsjvwbkdqyldhwyhwkhf4y23aqq7jayd[.]onion	C2 domain 2022
bihgkrr546ctjdn4mwr7x4bhvwz55sftx6xir6cwlfo6rhppd2eu7syd[.]onion	C2 domain 2022
2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad[.]onion	C2 domain 2022
c43tnmrkzfmkjyd3j4v6xbyrd67q6pskzy67dwkzj36uoqwpoju2loyd[.]onion	C2 domain 2022
2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad[.]onion	C2 domain 2022
yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad[.]onion	C2 domain 2022
dg2sz7pxs7llf2t25fsbutlvvrjij4pmojugn75cmxnvoshmju6dzcad[.]onion	C2 domain 2022
c43tnmrkzfmkjyd3j4v6xbyrd67q6pskzy67dwkzj36uoqwpoju2loyd[.]onion	C2 domain 2022

IOC	Description
2pkktxkf3gnpcjh2bhi62arz2ieyjgxocb3jne3kc2nu2yvyxqq23nad[.]onion	C2 domain 2022
papmcl4r32awafck75y5446n252qqqq4h6c4y2slaayposrtfbcebdqd[.]onion	C2 domain 2022
maesvpovrwqfaqjw44bbeb2w62h6n7eyosbeit7rfrrdbyjymqaxfryd[.]onion	C2 domain 2022
yeug3c6mnwocixwlotka4nwo3fjtfic65o4psmpxvrdul5q7dgjmsvad[.]onio	C2 domain 2022 with a typo
7owe32rodnp3vnx2ekqncoegxolkmb3m2fex5zu6i2bg7ktivhwvczqd[.]onion	C2 domain 2021
r5vg4h5rlwmo6oa3p3vlckuvf5na2wb2tnqbsbkivhrhlyze6czlpjad[.]onion	C2 domain 2021
limeprime[.]com	Associated domain
greenphoenix[.]xyz	Associated domain
revouninstaller[.]homes	Associated domain
getyourgift[.]life	Associated domain
12EfzLra6LttQ8RWvBTDzJUjYE6eRxx4TY	Wallet Address
14XZhcCJDguZuZF4p13tfLXJ6puudY7gqs	Wallet Address
15nWGFaodg3efVKATgsaaSPU2TxSbiMHcP	Wallet Address
19RzEN3pqHvgRHGMjjtYCqjVTXt8bnHkK3	Wallet Address
1AuWUMtjPo7Cc1Ji2pz7DWVvVJ5EjiUaHh	Wallet Address
1BL6NZSoXtMSdquRmePDUCQxFaXtLLSVWG	Wallet Address
1BqY56No1LR64AGcog4mF54UTPnjrPAPHz	Wallet Address
1BrEshrz6gVbVuHGBgJ5GuHBvC2sdoeTAJ	Wallet Address
1CfevVPC8cSpFf7QKQwShrFgQYfyQaoXhc	Wallet Address
1HzJkTn6Z5nDrgbR6dHVBDVtsRYqwDmGzN	Wallet Address
1KfLXEveeDEi58wvuBBxuywUA1V66F5QXK	Wallet Address
1LQ2EPBwPqdbmXwN6RodPS4xqcm8EtPcaB	Wallet Address
1MuJwQKLQKt1VCBQ9u1RtepW7sDD3AwRE6	Wallet Address
1Mz2b2onxnAYhJTJQoGHdSBy6wu2HpufVR	Wallet Address

IOC	Description
1NX7zTP6C4oGj2y3DaJTrg26AGFWExvYnr	Wallet Address
1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1	Wallet Address
1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97	Wallet Address
1HjoomvzjtvZdbznoEijTNAkMjmsFba9fY	Wallet Address
34RqywhujsHGVPNMedvGawFufFW9wWtbXC	Wallet Address
15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6	Wallet Address

Related Links:

- Blog: How IoT Botnets Evade Detection and Analysis – Part 1
- Blog: Could Threat Actors Be Downgrading Malware to Evade Detection?