IcedID Command and Control Infrastructure

silentpush.com/blog/icedid-command-and-control-infrastructure

April 25, 2021

Apr 25
Written By Ken Bagnall

Martijn March 31st 2021

First Published 31st March 2021 by Martijn

Earlier this week, the DFIR Report published an interesting analysis of an intrusion with the notorious SodinokibiREvil ransomware. The intrusion used IcedID as the initial access broker: many ransomware actors use another malware campaign to gain access to an internal network and IcedID has become a very popular choice for that.

In this blog post, I use the IOCs shared by the DFIR Report to uncover more command and control infrastructure linked to IcedID, some of which has not been published before.

IcedID, also known as Bokbot, was discovered by IBM X-Force in November 2017. Initially operating as a banking trojan, it has since made the same move that Emotet had made previously and is now used to serve a foothold within a network that is than later used by a ransomware operation.

The DFIR Report's analysis lists cikawemoret34[.]space and nomovee[.]website as IcedID command and control servers used during the intrusion. These domains were hosted on the IP addresses 206.189.10[.]247 and 161.35.109[.]168 respectively.

It is always a good idea to see what other domains were hosted on these IP addresses. Using Silent Push passive DNS data, on 206.189.10[.]247 I also found the following domains:

```
33nachoscocso[.]website
berxion9[.]online
chinavillage[.]uno
emanielepolikutuo1[.]website
gommadrilla[.]space
oskolko[.]uno
prolomstenn[.]fun
```

While on 161.35.109[.]168 I also found:

```
aspergerr[.]top
kneelklil[.]uno
newstationcosmo8[.]space
```

Unsurprisingly, most of these domains have been publicly linked to IcedID.

All the domains were registered through Porkbun in February or March and parked there initially before switching to Cloudflare's nameservers and pointing to the aforementioned IP addresses. This switching happened at different times for different domains, suggesting that the switch was made just before a domain was used in a campaign.

One domain stands out: emanielepolikutuo1[.]website first switched to using nameservers belonging to Russia's Server Space and pointing to the IP address 143.198.25[.]214, before switching to Cloudflare and 206.189.10[.]247 a little over a week later.

So, I had a look at 143.198.25[.]214 and found the following domains hosted there:

```
apouvtios2[.]uno
awefoplou5[.]site
chajkovsky[.]space
daserwewlollipop[.]club
dastemodaste[.]fun
emanielepolikutuo1[.]website
ohbluebennihill[.]website
seconwowa[.]cyou
violonchelistto[.]space
zomonedu3[.]website
```

All but one of these domains were registered at Porkbun, the exception is the slightly older seconwowa[.]cyou, which was registered through NameSilo.

Just like the previous set of domains, all these domains switched to using Cloudflare's nameservers at some point and switched IP addresses at the same time. However, some first pointed to 83.97.20[.]176 before pointing to 143.198.25[.]214. On the former IP addresses, I also found four more domains:

```
ameripermanentno[.]website
mazzappa[.]fun
odichaly[.]space
vaccnavalcod[.]website
```

Again, these used same pattern of registering at Porkbun before switching to Cloudflare's nameservers and the above IP address.

Of the latter two lists of domains, only some have been publicly linked to IcedID activity. However, the similarities noted above, as well as the choice of TLDs, make me confident these domains belong to the same infrastructure and either have been or will be used in IcedID campaigns.

There is a pattern there: a domain gets registered, usually at Porkbun, and parked there for a while before its nameservers switch to those of Cloudflare when the domain points to a new IP address. This IP address hosts multiple of these domains. There is also a preference for slightly unusual top-level domains.

Using this pattern, I dug into the Silent Push data trove to look for other domains that satisfied this pattern. I had to sift through the results to filter out false positives, but I ended up with a list of domain names and corresponding IP addresses of which I consider it very likely they belong to IcedID's infrastructure.

Many of these indicators have been published previously, for example on Maltrail's GitHub, but many others have not been publicly linked to IcedID before.

You can find the full list of 58 IP addresses and 323 domain names (and 402 combinations: some domain names have pointed to multiple IP addresses) on our GitHub page.

Conclusion

Malware like IcedID plays a crucial role in many large cybercrime campaigns, including ransomware, which can be very costly for the victim organization. Early knowledge of indicators is thus important, even if these indicators haven't all been publicly linked to the malware. In this blog post, I have shown how I was able to find hundreds of such indicators by spotting some patterns in the domain behaviour.

Thanks to John Jensen and Ken Bagnall for their contributions.

Subscribe

Ken Bagnall