Thawing IcedID Out through a DNS Analysis

Table of Contents

Executive Report

Evolution isn't only for humans and other living things. Apparently, malware can evolve, too, and IcedID is a good example.

First detected as a banking trojan in 2017, IcedID continues to undergo updates that make it even more dangerous. In the past few months, IcedID variants have been observed to deliver ransomware payloads instead of performing its original function—stealing financial data.

Another notable change was that victim hosts now connect to the IceID command-and-control (C&C) servers using port 443 instead of 8080, making the action harder to detect. These latest activities inspired Cymru researchers[1] to continuously track and analyze the IcedID BackConnect Protocol. In a recent report, they listed 34 IP addresses that pointed to the malware's C&C servers, namely:

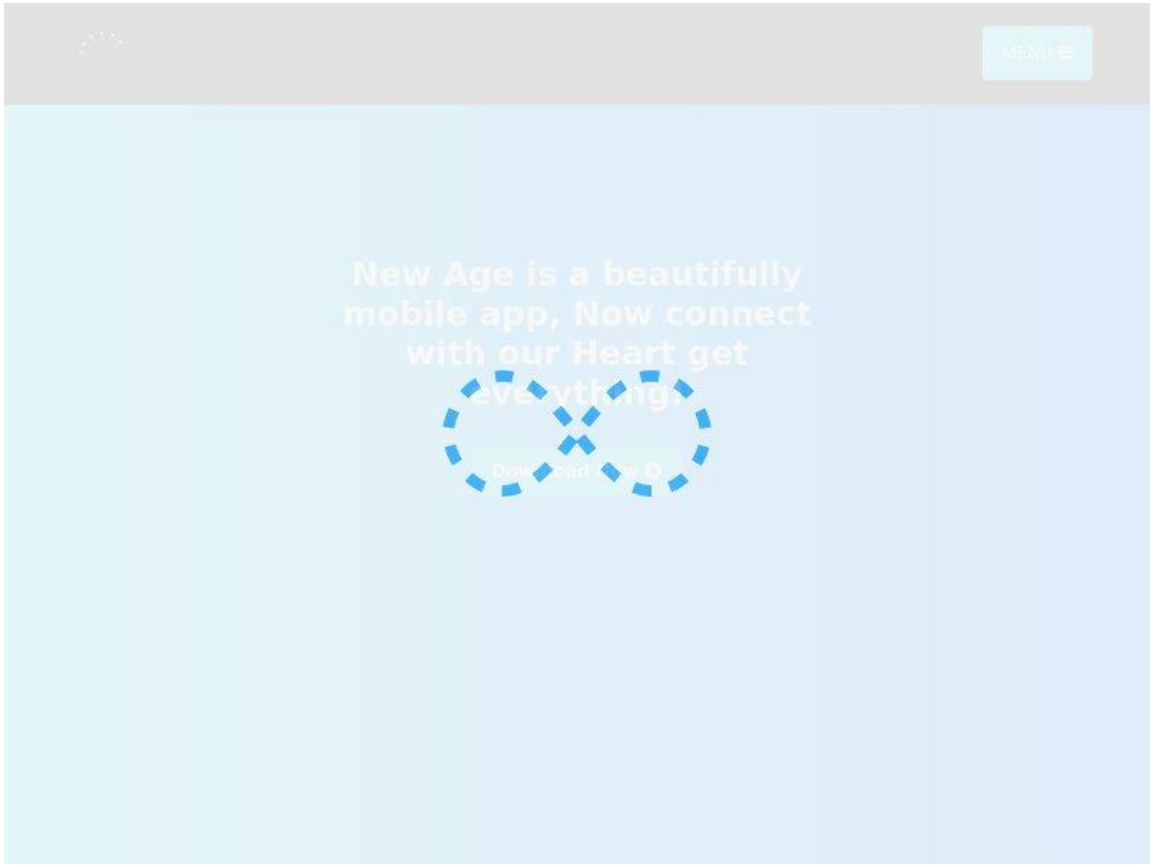
- 5[.]196[.]196[.]252
- 135[.]148[.]217[.]85
- 80[.]66[.]88[.]71
- 45[.]61[.]137[.]220
- 193[.]239[.]85[.]16
- 185[.]99[.]132[.]16
- 167[.]99[.]235[.]95
- 162[.]33[.]179[.]145
- 46[.]21[.]153[.]153
- 193[.]149[.]176[.]100
- 45[.]61[.]139[.]144
- 45[.]61[.]137[.]159
- 45[.]61[.]139[.]235
- 193[.]149[.]176[.]198
- 192[.]153[.]57[.]134
- 193[.]149[.]187[.]7
- 162[.]33[.]179[.]218
- 139[.]59[.]33[.]128
- 138[.]197[.]146[.]18
- 167[.]99[.]248[.]131
- 134[.]122[.]62[.]178
- 104[.]248[.]223[.]35
- 64[.]227[.]48[.]93
- 209[.]38[.]220[.]183
- 161[.]35[.]166[.]97
- 138[.]68[.]244[.]54
- 68[.]183[.]198[.]18
- 207[.]154[.]203[.]203
- 64[.]227[.]146[.]71
- 116[.]203[.]30[.]206
- 139[.]59[.]186[.]140
- 139[.]59[.]72[.]105
- 104[.]248[.]21[.]165
- 159[.]89[.]116[.]11

WhoisXML API researchers also found more indicators of compromise (IoCs) listed on three AlienVault OTX pulses,[2,3,4] adding nine IP addresses and 15 domains to the list. Our analysis and expansion of the IoC lists led to these key findings:

- Five unredacted email addresses historically used to register some of the domains identified as IoCs
- 44 domains currently registered using the email addresses
- 22 domains resolving to some IP addresses tagged as IoCs
- 33 domains sharing the same IP resolutions as some of the domains classified as IoCs
- 14% of the artifacts were flagged as malicious by a bulk malware check

IcedID IoCs: What We Know So Far

We subjected all 43 IP addresses tagged as IoCs to a bulk IP geolocation lookup and found that all except 45[.]61[.]137[.]159 had active resolutions. They were primarily managed by Digital Ocean (40%) and BL Networks (21%). Several of them also pointed to live pages. Take a look at some of them below.



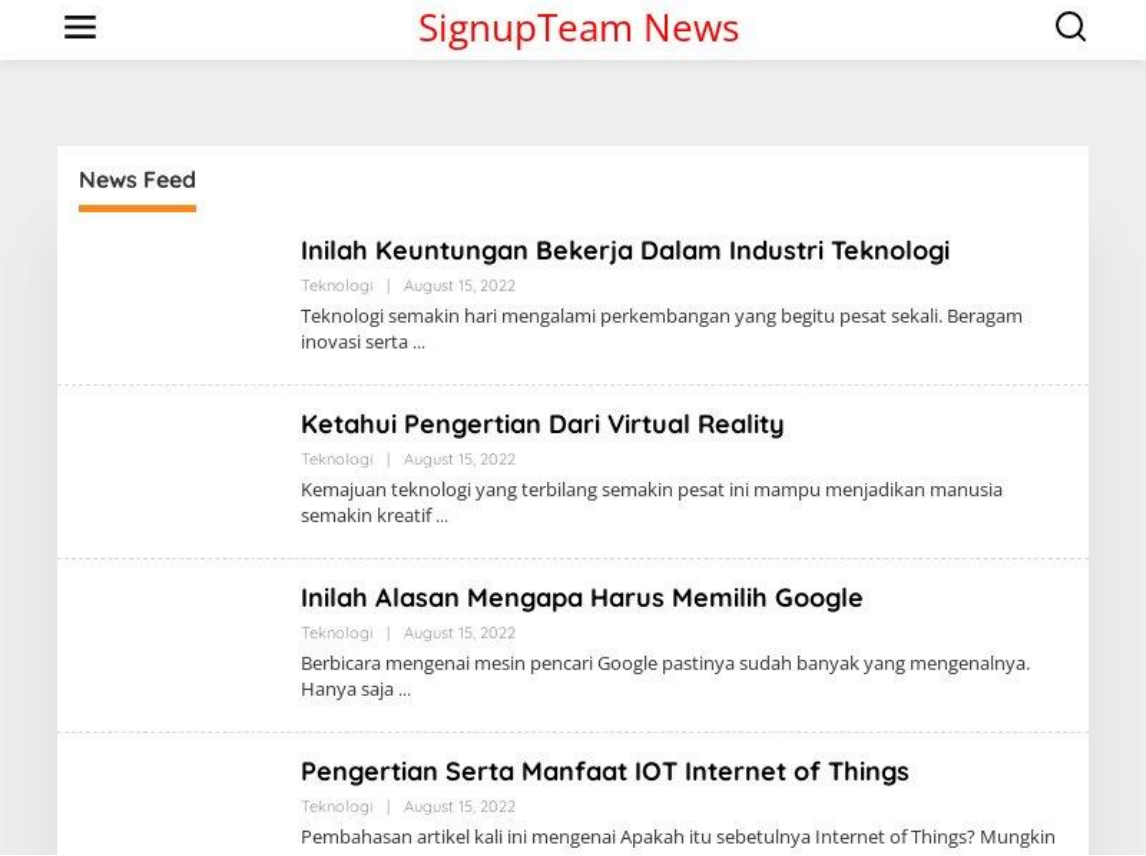
Screenshot of 116[.]203[.]30[.]206, resolving to on-mail[.]ru

Screenshot of 139[.]59[.]33[.]128

On the other hand, the domains tagged as IoCs by AlienVault told a different story. Only one out of the 15 domains had current WHOIS records—2fgithub[.]com, which uses Perfect Privacy LLC as its WHOIS privacy protection provider.

Upon further investigation, we found that some of the domains continued to host or redirect to live pages.

Screenshot of click[.]org



Screenshot of signup[.]team

Mapping Out IoC Connections

We dug deeper into the IcedID infrastructure in hopes of finding more related properties that may not have been identified yet. The threat actors may have inadvertently left traceable artifacts. They could also be waiting to use some of them in the future or may already be doing so.

Identifying IP Connections

Reverse IP lookups for all of the IP addresses tagged as IoCs revealed that only 12 had resolving domains. Each was connected to only four or fewer domains, indicating a dedicated IP network. In total, we found 22 unique domains resolving to the malicious IP addresses.

Examining the Domains Identified as IoCs

We looked into the malicious domains' historical WHOIS records to see if other digital properties were connected to them. This led us to five unredacted email addresses, two of which were used to register more than 50 domains and therefore could be owned by a

domainer. Thus, we decided to focus on the 44 connected domains registered using the remaining three email addresses.

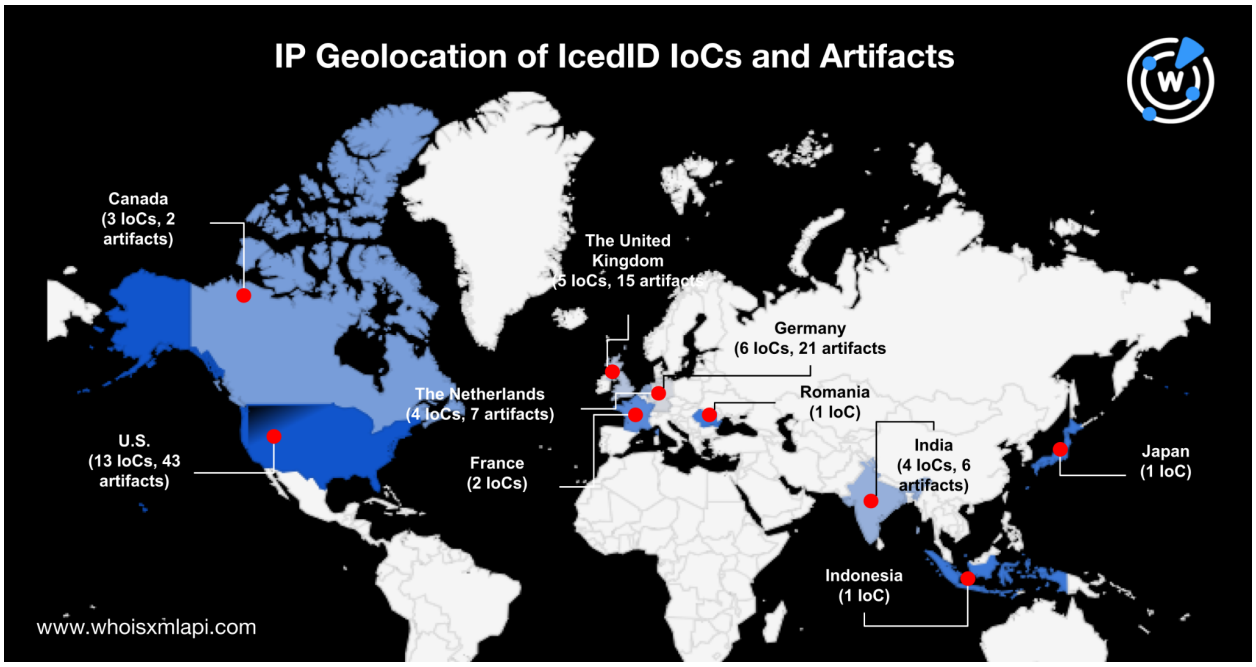
We also looked at the IoCs' IP resolutions and found that only six out of the 15 led to live content. Three of them shared their IP addresses with more than 250 other domains. That left us with 33 domains with a higher probability of being part of or connected to the malicious domain network.

A Closer Look at the Artifacts

In total, we identified 99 probable IP- and domain-connected artifacts. About 14% of them have been classified as malicious.

We also ran a bulk WHOIS lookup for the connected domains and found that only 53 had current WHOIS records with Domain Cost Club as registrar.

Their IP geolocation lookup results revealed that they were spread out across seven countries, including those that were either close to or the country locations of the IP addresses the Cymru researchers named. The map below shows these countries.



—

From an initial list of 59 IoCs, the DNS bread crumbs IceID left led us to 99 additional domains that could be part of or connected to the threat's infrastructure. The artifacts' connection to the IoCs may warrant further scrutiny and suspicion.

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.*

Appendix: Source, Sample Artifacts, and IoCs

Sources

[1] https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol-part-2
[2] https://otx.alienvault.com/pulse/64cb26ac4990112e3f9e662f
[3] https://otx.alienvault.com/pulse/64c5cf320a92c0bdc8ab9068
[4] https://otx.alienvault.com/pulse/6401246d57e5b0d2ff1c6c58

Sample IoC IP Resolutions

- 1[.]23[.]82[.]72
- 104[.]248[.]21[.]165
- 104[.]248[.]223[.]35
- 106[.]177[.]224[.]34
- 116[.]203[.]30[.]206
- 134[.]122[.]62[.]178
- 135[.]148[.]217[.]85
- 138[.]112[.]25[.]25
- 138[.]197[.]146[.]18
- 138[.]68[.]244[.]54
- 139[.]59[.]186[.]140
- 139[.]59[.]33[.]128
- 139[.]59[.]72[.]105
- 159[.]89[.]116[.]11
- 161[.]35[.]166[.]97
- 162[.]33[.]179[.]145
- 162[.]33[.]179[.]218
- 167[.]99[.]235[.]95
- 167[.]99[.]248[.]131
- 185[.]99[.]132[.]16
- 192[.]153[.]57[.]134
- 193[.]149[.]176[.]100
- 193[.]149[.]176[.]198
- 193[.]149[.]187[.]7
- 193[.]239[.]85[.]16
- 2[.]12[.]51[.]56
- 207[.]154[.]203[.]203
- 209[.]38[.]220[.]183
- 21[.]15[.]46[.]55
- 35[.]3[.]46[.]245
- 36[.]75[.]75[.]75
- 45[.]61[.]137[.]159

- 45[.]61[.]137[.]159
- 45[.]61[.]137[.]220
- 45[.]61[.]139[.]144
- skigimeetroc[.]com
- skansnekssky[.]com
- askamoshopsi[.]com
- submit[.]org
- signup[.]team
- repository[.]click
- continue[.]email
- click[.]zero
- click[.]talk
- click[.]org
- click[.]open
- click[.]discover
- click[.]contact
- click[.]compare
- 2fgithub[.]com

Sample IP-Connected Domains

- bortolatolino[.]it
- bxbotel[.]expert
- delivery-pt[.]com
- lfctoken[.]live
- liverpoolfctoken[.]club
- liverpoolfctoken[.]com
- liverpoolfctoken[.]online
- luisianafox[.]com
- mail[.]on-mail[.]ru
- nexus-api[.]scoutabroad[.]com
- gabrikxuira[.]com
- gyxplonto[.]com
- iskazorety[.]com
- keyzishaptu[.]com
- minesotkarpid[.]com
- nemchaprues[.]com
- pichervoip[.]com
- pinchersoftqum[.]com
- satifayban[.]com
- skansnekssky[.]com

Sample Email-Connected Domains

- xn--qei8618m[.]ws
- xn--hl8haa[.]ws
- dcchosting1[.]ws
- xn--xj8haa[.]ws
- xn--k78h[.]ws
- emojis[.]ws
- xn--fz7h[.]ws
- xn--5h8h[.]ws
- whassup[.]ws
- xn--qei2808m[.]ws
- wassup[.]ws
- xn--57h9759n[.]ws
- xn--5l8haa[.]ws
- usa-merchant[.]com
- wesmile[.]ws
- worksuccess[.]ws
- xn--57hz0a[.]ws
- emojidomain[.]ws
- get-a-name[.]com
- geekwear[.]co

Sample Malicious Artifacts

- dcchosting1[.]ws
- delivery-pt[.]com
- troptionstrading[.]com
- minesotkarpid[.]com
- nemchaprues[.]com
- pichervoip[.]com

- pinchersoftqum[.]com
- satifayban[.]com
- skansnekssky[.]com
- softwinmeod[.]com
- startinghpot[.]com
- troffyfrutlot[.]com
- yhorneedminf[.]com
- abigelofraj[.]com