A Visualizza into Recent IcedID Campaigns:

team-cymru.com/post/a-visualizza-into-recent-icedid-campaigns

S2 Research Team

October 7, 2022

Reconstructing Threat Actor Metrics with Pure Signal™ Recon

Introduction

IcedID (also known as BokBot) started life in early 2017 as a banking trojan that later evolved to include dropper malware capabilities. These capabilities enable IcedID to download and deploy additional malware like Cobalt Strike, with recent infections leading to Quantum ransomware. Cybersecurity professionals should continue to pay attention to IcedID as it remains one of the top dropper malware in the threat landscape and has no signs of slowing down. It is typically delivered via email spamming campaigns, with new campaigns being delivered on a near-daily basis that leverage an assortment of different lure types and execution processes.

This got us curious - how do different campaigns compare to each other? We've extensively tracked IcedID C2 infrastructure using our Recon and BARS (Botnet Analysis and Reporting Service) feed tooling, and using this data we were able to peek behind the scenes at metrics that are possibly similar to what the threat actors are tracking themselves.

C2 Tracking

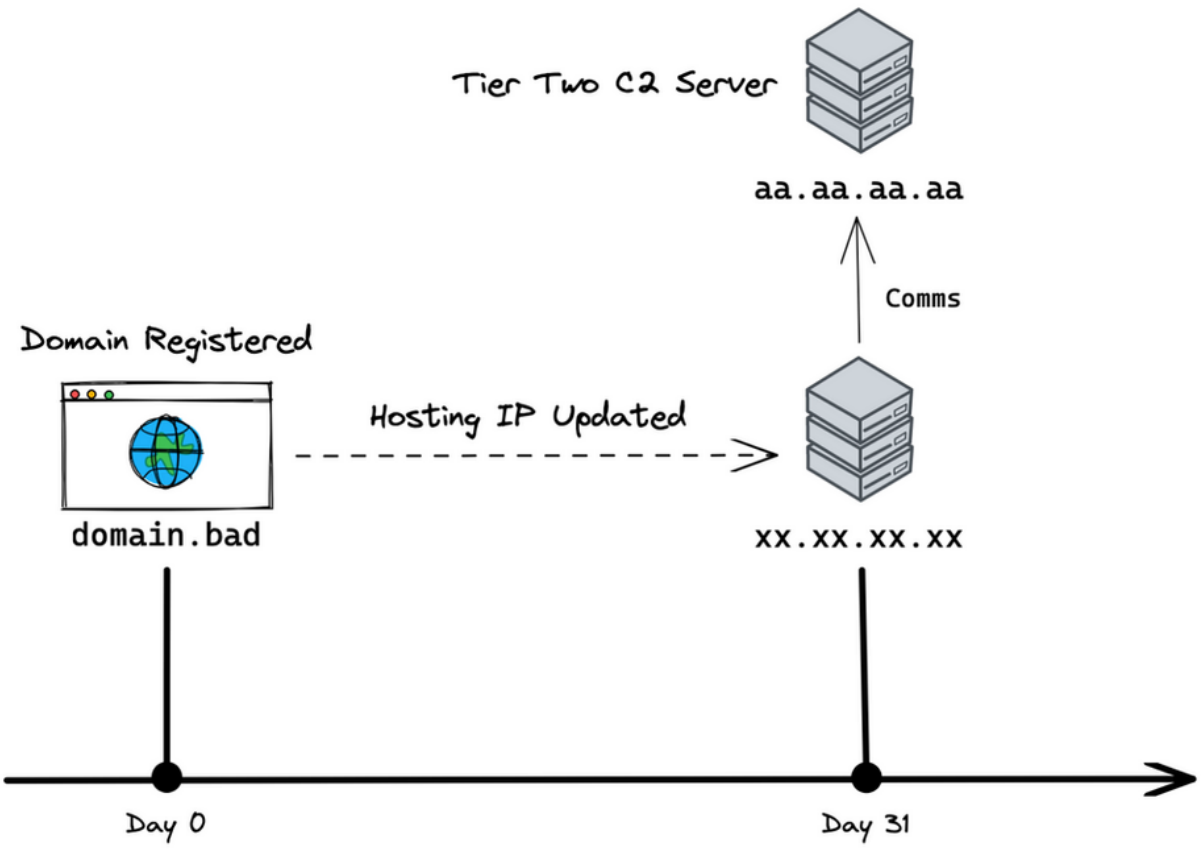
We've previously written about IcedID Stage 2 Tier 1 (T1) and Tier 2 (T2) C2 infrastructure and threat telemetry, which pertains to bot activity that occurs after IcedID has successfully infected a machine. In this post, our focus is on the Stage 1 T1 C2s that initially load the malware onto a victim's machine after they perform the action being asked of them in the lure, such as 'enable macros' or 'click a disguised shortcut'.

Registration

Until 21 September 2022 and dating back to at least two months, domains used as Stage 1 downloader C2s were registered with 1337 Services LLC Hosting (connected to the Njalla hosting service) and parked there for an average of 31 days before use as a C2. This process was possibly developed for the circumvention of firewall blocks against newly registered domains. As of 22 September 2022, however, domains used as C2s have been registered only a few days prior, breaking this long-term pattern.

C2 Assignment

Either the day before or the day of a campaign, a C2 domain is assigned to a new IP that is used for inbound victim traffic on port 80 and for T1 -> T2 communications. Communication with the T2 C2 generally begins the same day the campaign is released.



According to our C2 tracking data for the August-September 2022 timeframe, domains and IPs are typically only used for one campaign and not recycled. In mid-September there were a few instances where downloader IPs and domains were reused, but as of the end of September, C2s have returned to being unique / single-use.

C2 Lifespan

C2 communication with T2 infrastructure occurs for an overall average of six days before ending, and four or five C2 IPs are normally active at a time. Although, around the third week of September active C2s dwindled down to two from the usual amount due to IPs and domains being reused between campaigns, which prevented aged-out C2s from being replaced. In most cases, no changes are made regarding the IP or domain once it’s inactive. All but one of the C2 domains from the campaigns we analyzed were still assigned to the same IPs at the time of writing.

Campaign Metrics

Using the C2s we've gathered from tracking IcedID infrastructure, we analyzed data from campaigns that were spammed during the period 13 - 21 September 2022 to see if there was a correlation between TTPs and the volume of victim interaction.

In order to identify potential traffic, we had to remove general noise, as well as security research traffic from our data. This process includes enrichment with supplementary open source data such as WHOIS information. The numbers provided throughout this blog are based on an approximation derived from sampled threat telemetry.

Delivery Methods

Of the campaigns analyzed, the following methods were used for malware delivery:

Password Protected ZIP -> ISO -> LNK -> JS -> [CMD or BAT] -> DLL

Delivery was via a password protected zip file that contained an ISO which itself contained a LNK file and archive holding the files used for IcedID installation. When the LNK file is clicked by the user, it functions as a shortcut to run a script within the archive that ultimately installs IcedID from a DLL. It is typically launched through either a CMD or BAT script, depending on which was included in the archive.

Password Protected ZIP -> ISO -> CHM -> DLL

Delivery was via a password protected zip file containing an ISO that led to a CHM (Compiled HTML) file. The victim must open the file to launch the DLL and complete the infection process.

Maldoc

Users received either a malicious Word or Excel file that asked them to enable macros, which then allowed the embedded script to execute and install IcedID.

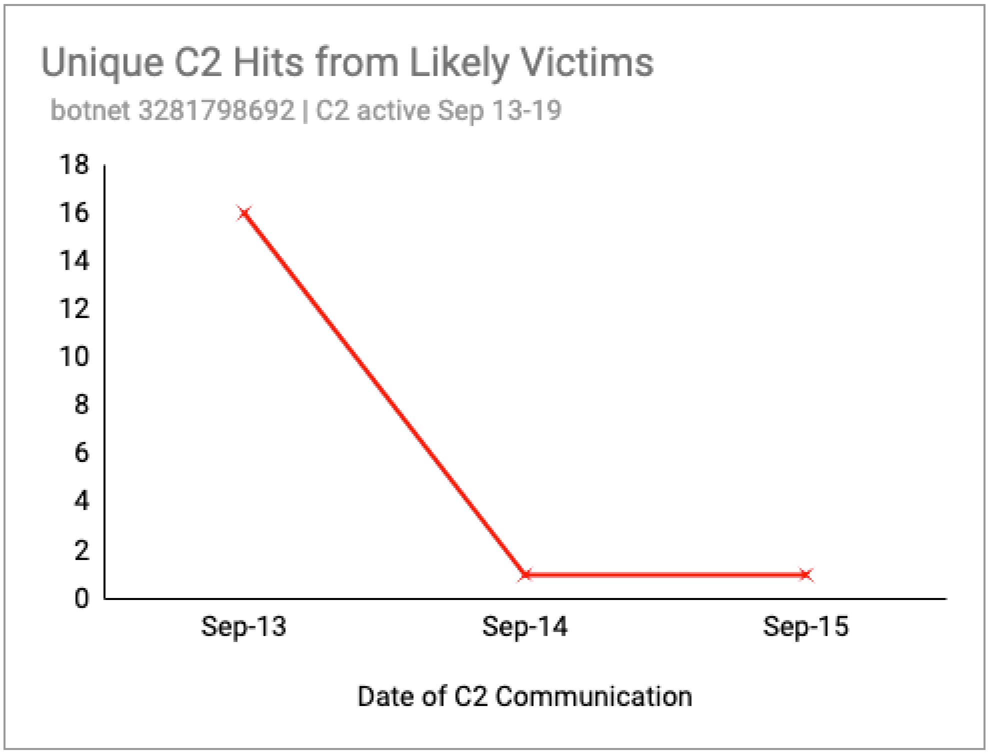
PrivateLoader

Delivery was through PrivateLoader, a pay-per-install service that distributes malware by hiding it in free software downloaded by unsuspecting users.

13 September

There were two campaigns launched; one targeting Italian speakers (project ID 3281798692) and the other targeting English speakers (project ID 726442267).

The Italian lure was in the form of a malicious '.docm' file with kolinandod[.]com as the C2, which was set to resolve to 159.203.5[.]238 on 12 September.

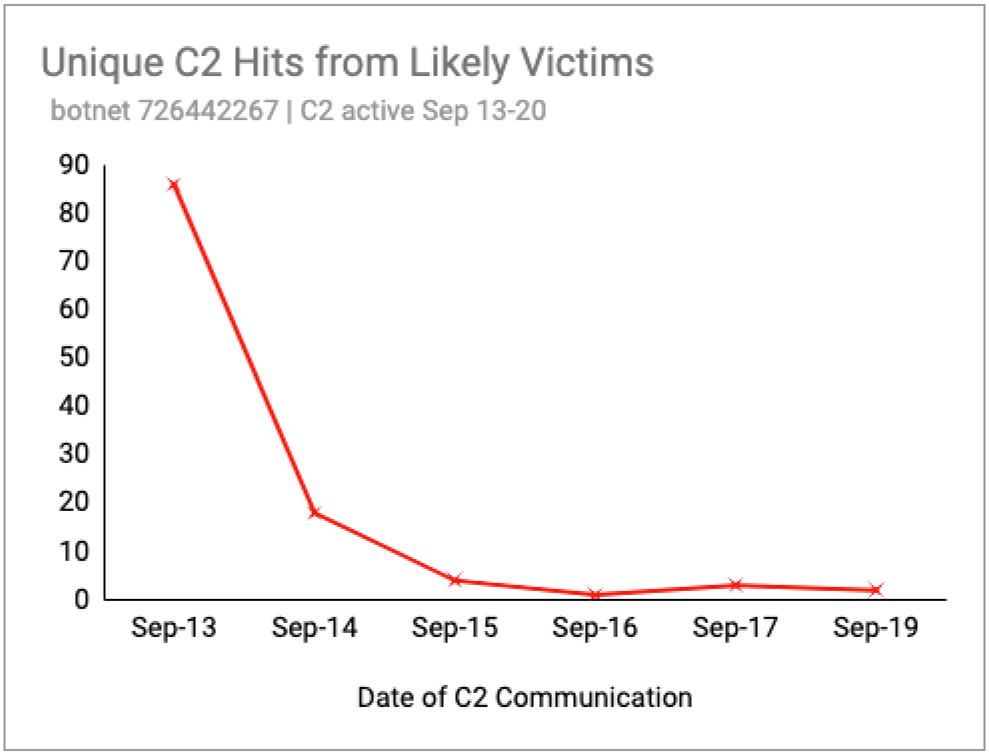


There were around 18 potential victims and most of the victim communication occurred the same day of the campaign. The C2 stopped interacting with the T2 on 19 September.

The lure targeting English speakers arrived using the following delivery method:

Password Protected ZIP -> ISO -> LNK -> JS -> BAT -> DLL

The C2 was qvantumbrakesz[.]com, which resolves to 134.209.97[.]90.



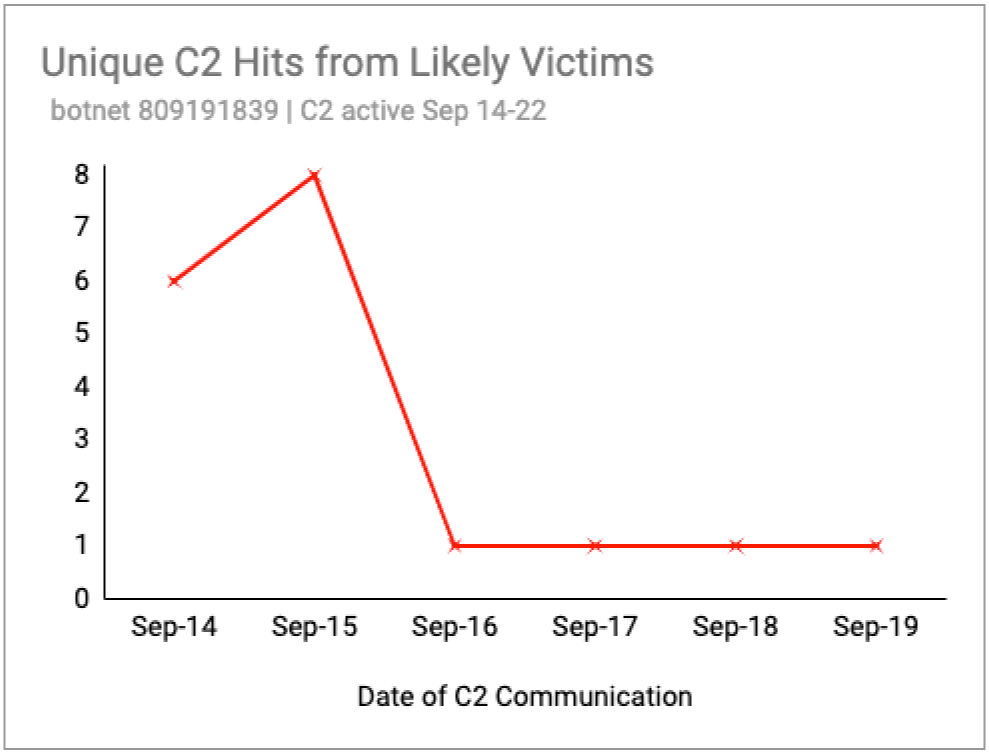
There were around 115 potential victims that communicated with the C2 before it was disconnected from the T2 on 20 September. Most of this traffic occurred on the day of the campaign and tapered off until the last victim hit it on 19 September.

14 September

For the campaign on 14 September (project ID 809191839), threat actors returned to leveraging CHM files for the delivery method:

Password Protected ZIP -> ISO -> CHM -> DLL

Note: The use of CHMs was first spotted in a IcedID campaign on 8 August 2022, but the use of this file-type maliciously is a technique that has been around for several years.



The C2 was allozelkot[.]com and was set to resolve to 188.166.169[.]40 on the day of the campaign. There were around 18 unique victims with the last connections occurring on the 19th. The C2 stopped communicating with the T2 on 22 September.

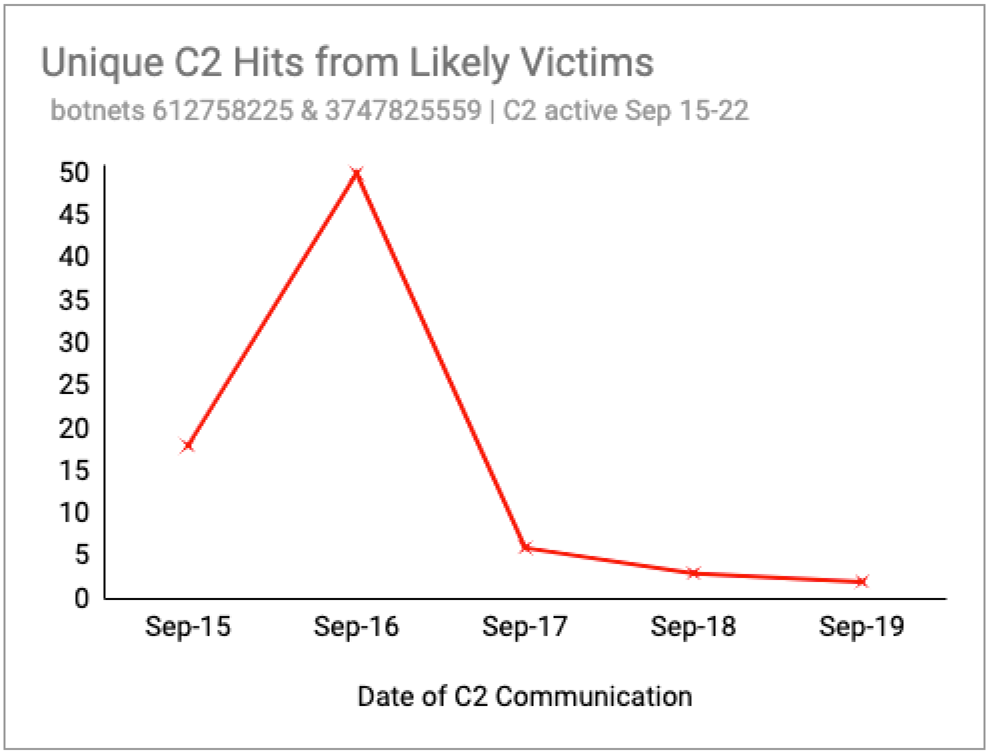
15-16 September

Both the 15 September and 16 September campaign used pildofraften[.]com as their C2. This domain has resolved to the same IP address (142.93.44[.]94) since 15 September. Seeing domains and IPs reused for Stage 2 bot C2s is not uncommon, but this is the first case of a Stage 1 downloader C2 reusing either since at least mid-August 2022.

The campaign on September 15 (project ID 612758225) used the delivery method:

Password Protected ZIP -> ISO -> LNK -> JS -> BAT -> DLL

The second campaign (project ID 3747825559), seen on 16 September, was delivered as an EXE dropped by PrivateLoader.



There were around 79 potential victims and most of them first communicated with the C2 on 16 September. The last victim requests to the C2 occurred 19 September and traffic with the T2 ended 22 September.

19 Sep

The campaign that occurred on 19 September (project ID 775636601) was a bit of an outlier compared to the others we've looked at so far. Delivery consisted of a password protected zip file containing an ISO:

Password Protected Zip -> ISO -> LNK -> DLL

The C2 was aviadronazhed[.]com, which was updated to resolve to 67.205.169[.]96 on the day of the campaign. Inbound port 80 traffic began at around 15:00 UTC and continued for about three hours for a total of five potential victims. T2 traffic began about two and half hours after the victim traffic (17:30 UTC) and lasted around two and half hours after the last port 80 request (20:30 UTC). Oddly, the C2 was then disconnected from the T2 instead of continuing to communicate for the usual period of approximately six days.

Another oddity was that unlike other C2s where domains remained on the same IPs at the conclusion of a campaign, this domain was updated and removed from 67.205.169[.]96 on 22 September.

20-21 September

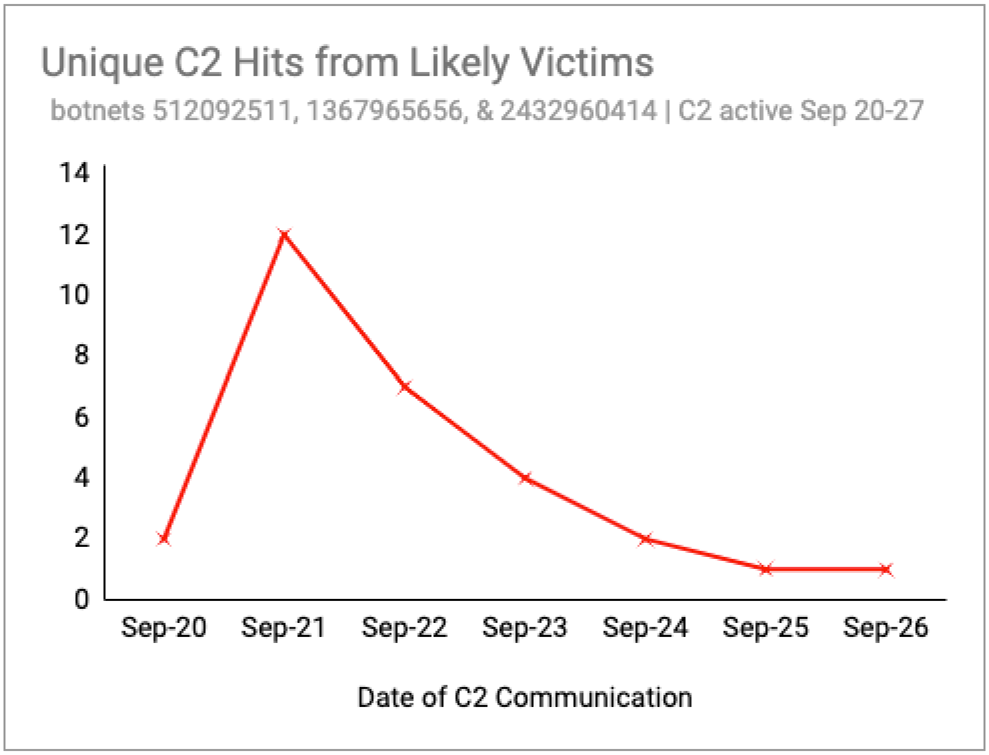
Three campaigns occurred during the period 20 - 21 September and each had a unique domain that resolved to the same IP (161.35.110[.]54). The IP was reused between domains similarly to the 15 - 16 September campaigns, except in this case the domains were unique.

There was one campaign seen on 20 September (project ID 512092511) with alkaliodplus[.]com as its C2. For delivery it used a password protected zip file and ISO:

Password Protected ZIP -> ISO -> LNK -> BAT -> DLL

Two campaigns were seen on 21 September, each with a unique project ID and domain: nikolandfantazy[.]com (project ID 1367965656) and zalikomanperis[.]com (project ID 2432960414). The delivery was via a password protected zip containing an ISO:

Password Protected ZIP -> ISO -> LNK -> JS -> CMD -> DLL



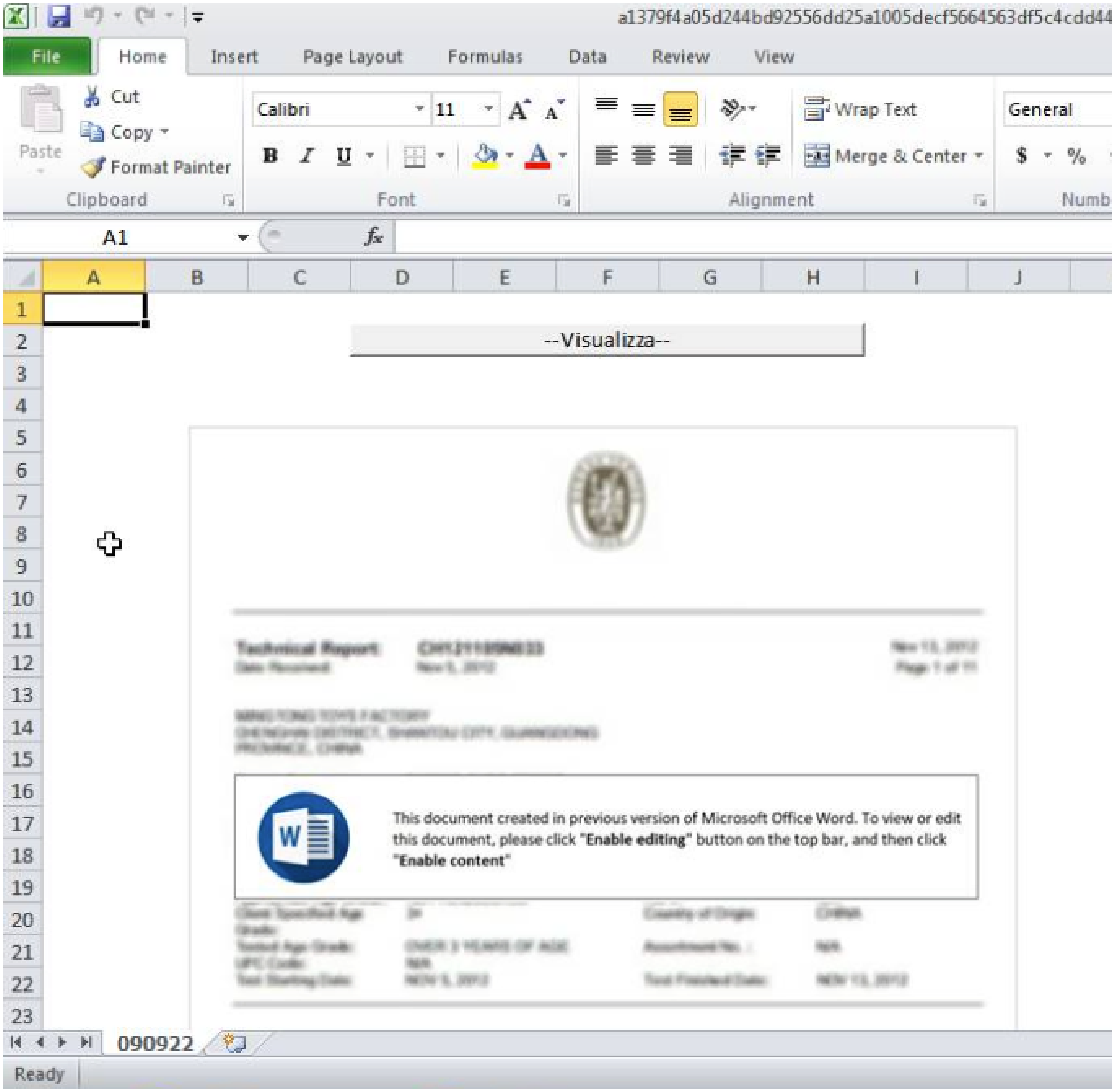
There were 29 potential victims from when the C2 was active between 20 - 27 September, with the last communication from a unique IP on port 80 happening on the 26 September. Only two victims hit the C2 on 20 September and most of the traffic began on 21 September before gradually tapering off.

Bonus Bloopers!

These campaigns fell outside of the timeframe we were focusing on but due to their peculiarities we thought it would be interesting to add for comparison.

9 September

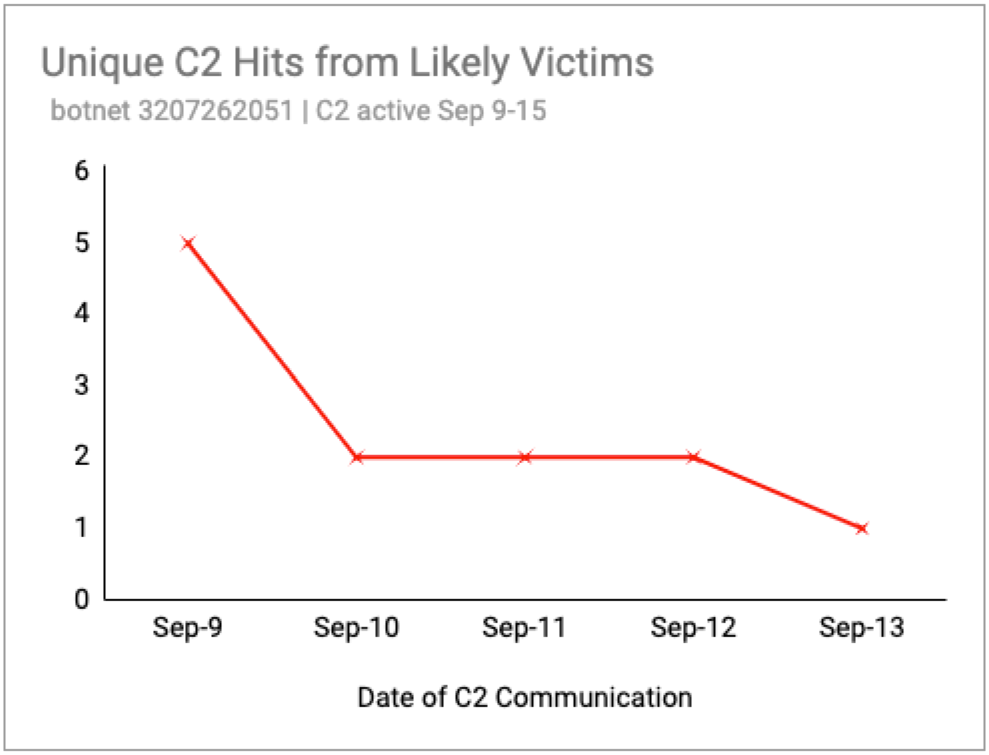
The lure for this campaign (project ID 3207262051) was meant to be an XLSM file for English-speakers, but the threat actors used the Italian word for “View” on the button they wanted to convince users to click.



This document created in previous version of Microsoft Office Word. To view or edit this document, please click "**Enable editing**" button on the top bar, and then click "**Enable content**"

Figure 1 – Screenshot from Hatching Triage

The C2 for this campaign was audifastinggip[.]com and it began resolving to 143.198.178[.]0 on 9 September.



Until 13 September around 12 potential victims were curious enough to click the “Visualizza” button, and communication with the T2 ended on 15 September.

22-23 September

It appears a key component of the process may have been skipped when setting up the C2 on 22 September (project ID 1023645195). The C2 was trallfasterinf[.]com, and it resolves to 137.184.114[.]20. Unlike the other C2s we’ve tracked which were registered an average of 31 days prior to being used in a campaign, this domain was the first to be registered only one day before it was a C2. It was assigned to this IP the day of the campaign, which is normal, but T2 communications appear to have never been set up. Potential victim traffic is hitting the C2, but it goes nowhere.

The C2 for 23 September (project ID 2349072319) was sebdgoldingor[.]com, and it also resolves to 137.184.114[.]20. Reusing IPs for these C2s is a new behavior which occurred twice in the same week. It was also registered with Njalla on 21 September, two days prior. Interestingly, T2 communications were still not set up when this second campaign launched. Two campaigns seen the following Monday on 26 September contained the expected T2 traffic, so it appears the threat actors may have had a bit of a mishap with 137.184.114[.]20.

Analysis/Key Findings

GEO Targeting

The 13 September campaign targeting Italian speakers resulted in 18 potential victims. It was also the only campaign from our timeframe using a malicious Word document as the delivery method, which makes a true comparison difficult. The campaign that leveraged a CHM file along with an English-lure also had 18 potential victims. It’s probable that the target base for this campaign was larger than that aimed at Italian speakers (based on the prevalence of both languages), so 18 potential Italian victims may be considered a successful number to the threat actors.

Delivery Methods

The campaign with the highest potential victim count was the campaign targeting English speakers that was released the same day as the Italian campaign (13 September). It was delivered via the most common method; a password protected zip file containing an ISO, which contained a LNK file. The second most successful campaign was that which leveraged PrivateLoader on 16 September 16.

From our observations, it appears that campaigns leveraging CHM files are less successful, which could explain why we have only seen this technique being used twice. However, we do not have a complete picture - the number of victims may have been proportionately similar (or different) based on the number of users targeted. For example, it is possible the CHM file campaigns were tests against a smaller target base, in which case one might argue that they *were* successful.

Lastly, it appears end users are far less likely to fall for a lure if there are any errors within the aesthetics, as seen with the campaign on 9 September – security awareness training appears to pay off! Unfortunately, in the majority of cases, lures look quite realistic and don’t always contain obvious errors and misspellings.

Traffic Timeline

Excluding the 19 September campaign as an outlier, the majority of victim traffic hits the C2 the day after a campaign is first reported in the wild. This could be a coincidence due to the small dataset being examined, and therefore will be a topic we revisit after further tracking.

Communication with the T2 infrastructure ends at least one day after the last victim traffic, which lasted anywhere from three to seven days. Due to the small sample size, this is also something we will continue to keep an eye on for any emerging patterns.

The timeframe we examined was coincidently when many odd behaviors were being observed, including the changes with C2s being reused, the time between domain registration and C2 assignment shrinking, and the campaign on 19 September that was quickly cut short (among other observations not mentioned). We believe that the threat actors behind IcedID were either making changes to various infrastructure processes behind the scenes or were having technical issues during this time.

Conclusion

In this post we pulled back the curtain on IcedID campaign metrics and Stage 1 C2 infrastructure, to shed light on behaviors and details not often available. These metrics are numbers the threat actors are watching as well, and just like any other business may influence their future actions.

When it comes to delivery methods, daily campaigns often leverage emails containing password protected zip files and ISOs and perform comparatively well. The relative success of the campaign leveraging PrivateLoader infections, with the malware concealed within ‘cracked’ software downloads, makes this method something also worth watching.

The threat actors spamming IcedID are likely aware that lures with glaring mistakes and typos perform poorly compared to those that are more realistic, as we saw with the campaign on 9 September. Targets may not be as easily tricked by phishing emails nowadays, but in response the threat actors have adapted their methods to use lures that appear legitimate and don’t typically include errors. Make sure your company’s security awareness training has adapted too!

We hope that these findings provide benefit to the reader in a number of areas:

- Context on the cadence, volume, and impact of IcedID campaigns.
- Data points for the assessment of the effectiveness of IcedID delivery TTPs.
- Context for the aging out of IcedID C2 IP IOCs; whilst IcedID domains continue to resolve to these IPs, their communications with the T2 cease after approximately 6 days.
- Topics for security awareness trainings that reflect the current environment

IOCs

67.205.169.96	aviadronazhed[.]com
134.209.97.90	qvantumbrakesz[.]com
137.184.114.20	trallfasterinf[.]com sebdgoldingor[.]com
142.93.44.94	pildofraften[.]com
143.198.178.0	audifastinggip[.]com
159.203.5.238	kolinandod[.]com
161.35.110.54	alkaliodplus[.]com nikolandfantazy[.]com zalikomanperis[.]com
188.166.169.40	allozelkot[.]com