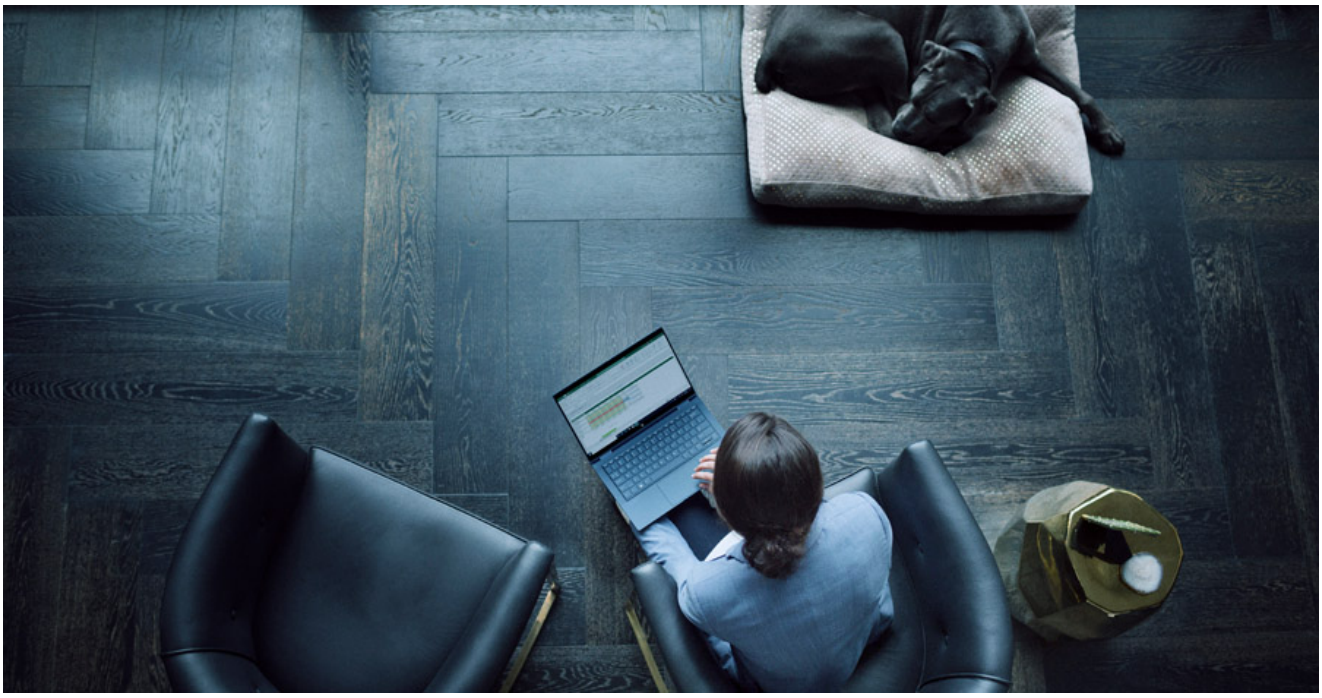
Recent Posts

threatresearch.ext.hp.com/mirrorblast-and-ta505-examining-similarities-in-tactics-techniques-and-procedures/

October 19, 2021

HP Threat Research Blog • MirrorBlast and TA505: Examining Similarities in Tactics, Techniques and Procedures



MirrorBlast and TA505: Examining Similarities in Tactics, Techniques and Procedures

What is MirrorBlast?

MirrorBlast is a new malware campaign first observed at the end of September 2021. The malware was named by Proofpoint Emerging Threats Labs, whose signatures recognize the malware based on its command and control (C2) traffic. Since then, the malware has been spotted in several campaigns, each showing similar infection chains. The following graphic shows the rough sequence of a MirrorBlast campaign.

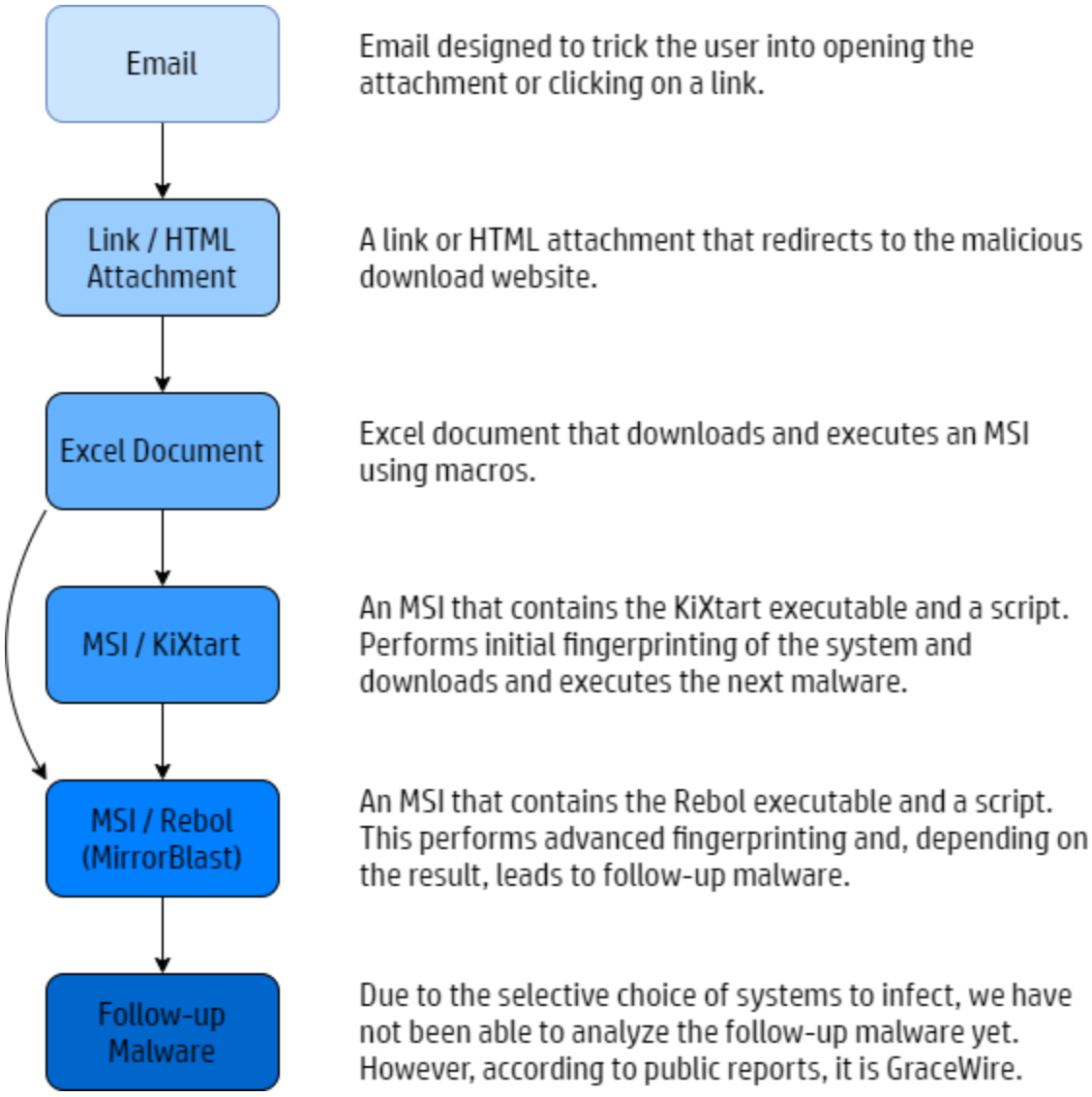


Figure 1 – Infection chain of a MirrorBlast campaign seen in October 2021.

Is MirrorBlast a campaign from TA505?

After MirrorBlast's emergence, some security researchers speculated that it could be linked to TA505. Comparing MirrorBlast activity to historical TA505 Get2/SDBBot campaigns revealed numerous similarities in tactics, techniques and procedures (TTPs). We assess that these similarities significantly strengthen the hypothesis that MirrorBlast and TA505 are linked. In this article, we describe some of these similarities:

- Similarities in modus operandi
- Similar domain registration patterns
- Campaign cadence
- Similar download websites and lure documents
- Similar target selection mechanisms
- Follow-up malware

Similarities in Modus Operandi

The Get2/SDBBot campaign TTPs were always similar, as if the group followed a strict playbook: The domains were registered, the download website was set up, and before the malware was distributed, the attackers uploaded a legitimate document to the download website. This was probably for testing purposes. Sometimes it was an empty document or one containing the characters “123”. But occasionally the attackers uploaded Excel documents containing several spreadsheets and legitimate content. For example, Figure 2 shows the test document that was uploaded during the Get2/SDBBot campaign on 14 September 2020.

Looking at the MirrorBlast campaigns, the threat actor behaved similarly. The campaign on 14 October 2021 was notable. Like TA505, the attackers registered domains, published the download website, and uploaded a test document. Strikingly, this test document was the same document as used by TA505 in a campaign in 2020, demonstrating an overlap in the attackers’ methods as well as the tools they use.

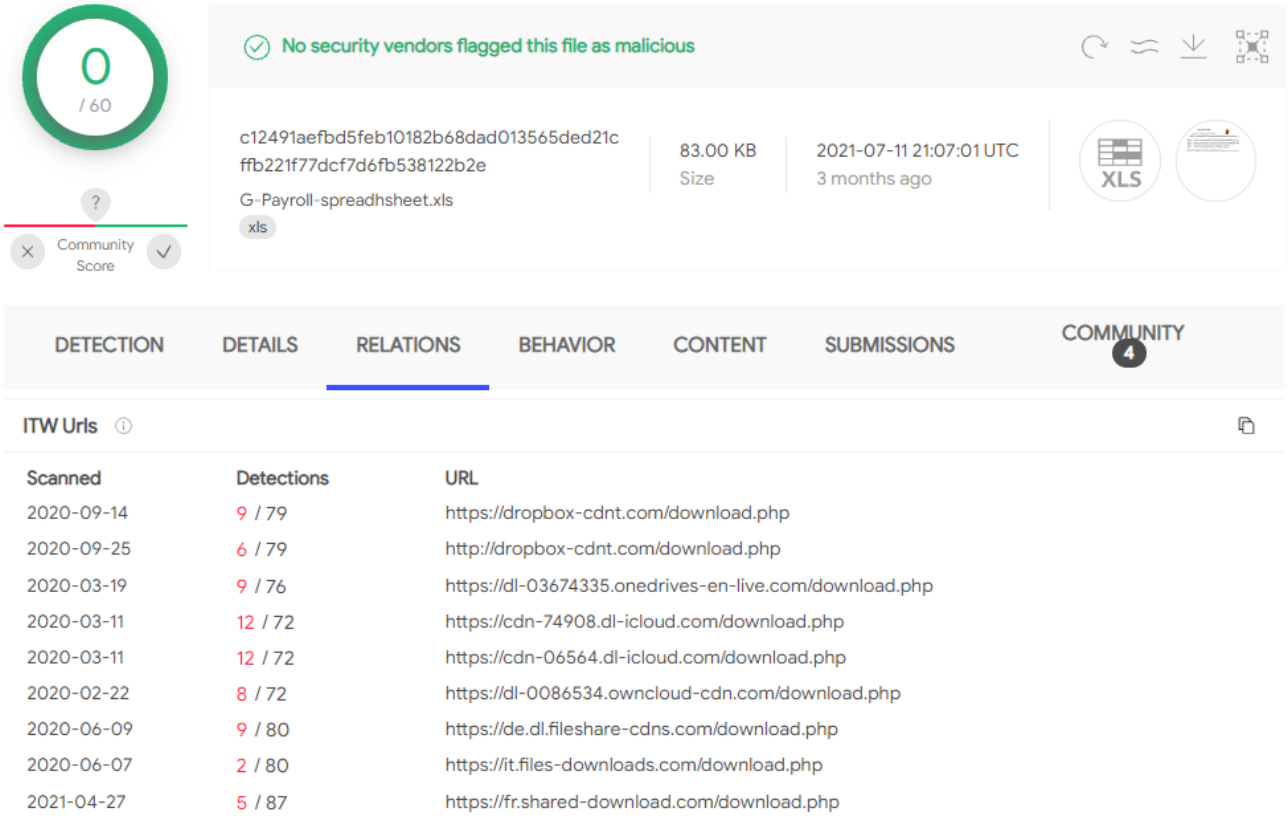


Figure 2 – Legitimate Excel file uploaded to TA505 and MirrorBlast malware distribution websites.

Similar Domain Registration Patterns

In Get2/SDBBot campaigns, TA505 registered new domains that had recognizable characteristics:

- Most domains impersonated well-known online services or used related keywords
- The domains often contained one or more hyphen characters to separate words
- The domains used the top-level domain *.com*

Here are some examples of known TA505 domains:

Known TA505 Domains
xbox-en-cnd[.]com
one-drive-storage[.]com
store-in-box[.]com
microsoft-store-drm-server[.]com
clouds-doanload-cnd[.]com
microsoft-sback-server[.]com
one-drive-ms[.]com
owncloud-cdn[.]com
cdn-onedrive-live[.]com
office-en-service[.]com

As you can see, the domains follow a consistent naming convention. Moreover, the combination of certain domain registrars and DNS service providers is also a good indicator of new TA505 domains. Figure 3 shows the domain registrars used in the documented TA505 campaigns from September 2019 to December 2020. Most of the time, Eranet International Limited was used to register the new domains and only rarely were others used. But in November and December 2020 this pattern changed when most domains were registered through Cnobin Information Technology Limited. After that, no more TA505 Get2/SDBBot campaigns ceased, resulting in no temporal overlap with MirrorBlast campaigns.

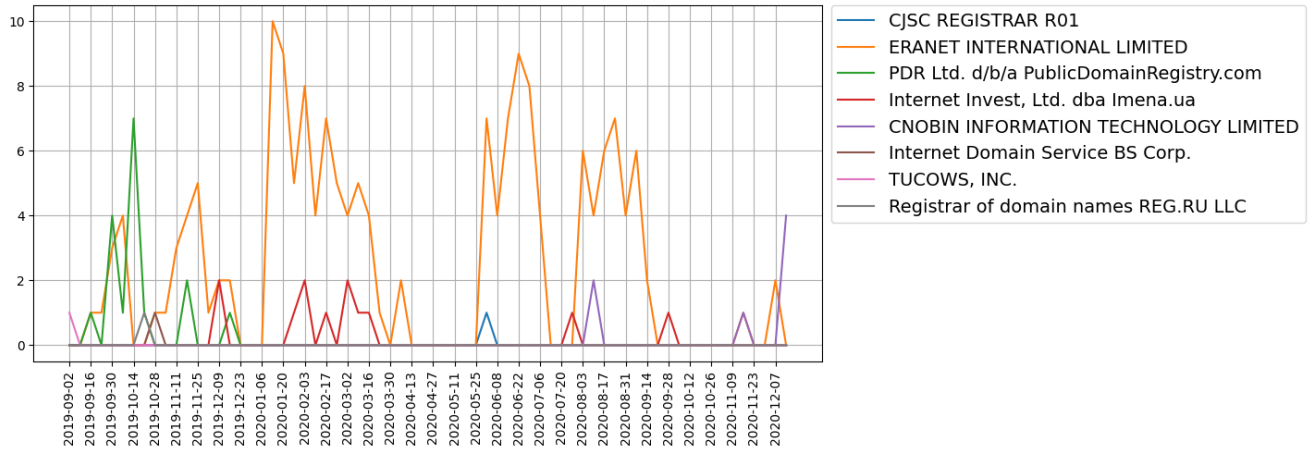


Figure 3 – TA505 domain registrations by registrar, September 2019 to December 2020.

As of October 2021, there are only a few known MirrorBlast domains. However, even the limited data suggest a consistent pattern in MirrorBlast domain registrations. As with TA505, the attackers imitate a well-known online service and often delimit keywords in their domains with hyphens. The threat actor behind the MirrorBlast campaigns used Cnobin Information Technology Limited to register their domains. This domain registrar was used by TA505 at the time of their last known activity in late 2020. There is no overlap in DNS service providers, since TA505 only used DNSPod and Cloudflare.

domain	created_date	registrar_name	name_server
feristoaul.com	2021-09-12T15:28:11+02:00	NICENIC INTERNATIONAL GROUP CO., LIMITED	["ns1.ndns.cn", "ns2.ndns.cn"]
fidufagios.com	2021-09-29T02:00:00+02:00	CNOBIN INFORMATION TECHNOLOGY LIMITED	["ns3.cnmsn.com", "ns4.cnmsn.com"]
cdn-8846-sharepoint-office.com	2021-09-30T02:00:00+02:00	CNOBIN INFORMATION TECHNOLOGY LIMITED	["ns3.cnmsn.com", "ns4.cnmsn.com"]
dzikic-my-sharepoint.com	2021-10-04T02:00:00+02:00	CNOBIN INFORMATION TECHNOLOGY LIMITED	["ns3.cnmsn.com", "ns4.cnmsn.com"]
dzikics-my-sharepoint.com	2021-10-04T02:00:00+02:00	CNOBIN INFORMATION TECHNOLOGY LIMITED	["ns3.cnmsn.com", "ns4.cnmsn.com"]
cdn03664-dl-fileshare.com	2021-10-06T02:00:00+02:00	CNOBIN INFORMATION TECHNOLOGY LIMITED	["ns3.cnmsn.com", "ns4.cnmsn.com"]

Figure 4 – MirrorBlast domain registrations.

Campaign Cadence

In 2020, TA505 ran a new campaign almost every day during the week. For this purpose, new domains were registered for Get2 and SDBBot distribution nearly every campaign. In addition, the spam waves of the campaigns were large. Comparing the cadence of MirrorBlast activity is difficult because of the limited data available at this point. However, comparing MirrorBlast activity to date suggests that the campaigns became more frequent at the end of September 2021 and currently match the cadence of TA505 campaigns. New domains are registered almost daily, which are used to spread malware.

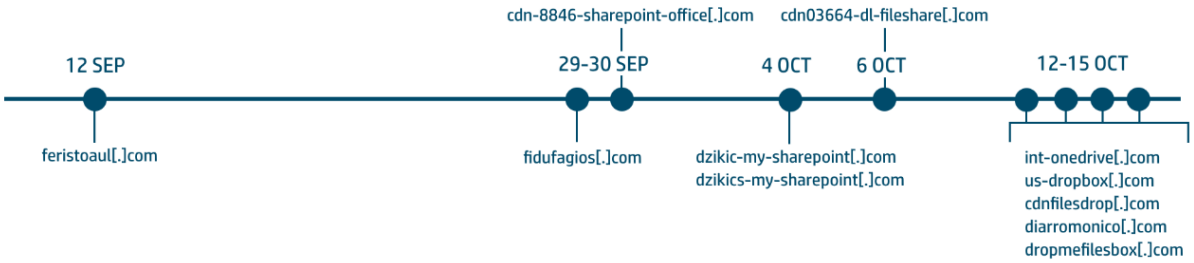


Figure 5 – Timeline showing MirrorBlast domain registrations from September to October 2021.

Infrastructure Overlap

In the MirrorBlast campaign on 4 October 2021, an overlap with known TA505 infrastructure was detected. The IP address 169.239.128[.]11, which pointed to the domain fidufagios[.]com in the MirrorBlast campaign, was previously used in a TA505 campaign on 9 October 2019. In the MirrorBlast campaign, the IP address was used for command and control (C2). Meanwhile, in the TA505 campaign, the IP address pointed to the domain onedrive-sdn[.]com and was used to host a malicious Excel document.

Campaign	Date	Domain	IP Address
MirrorBlast	4 October 2021	fidufagios[.]com	**169.239.128[.]11**
Get2/SDBBot (TA505)	9 October 2019	onedrive-sdn[.]com	**169.239.128[.]11**

Similar Download Websites and Lure Documents

Another similarity between the two campaigns is the design and use of websites to trick users into downloading malicious Excel spreadsheets. Both campaigns lead users to a download website via a hyperlink or an HTML attachment, whose design varies from campaign to campaign. Figure 6 shows the website of a Get2/SDBBot TA505 campaign from 14 February 2020.

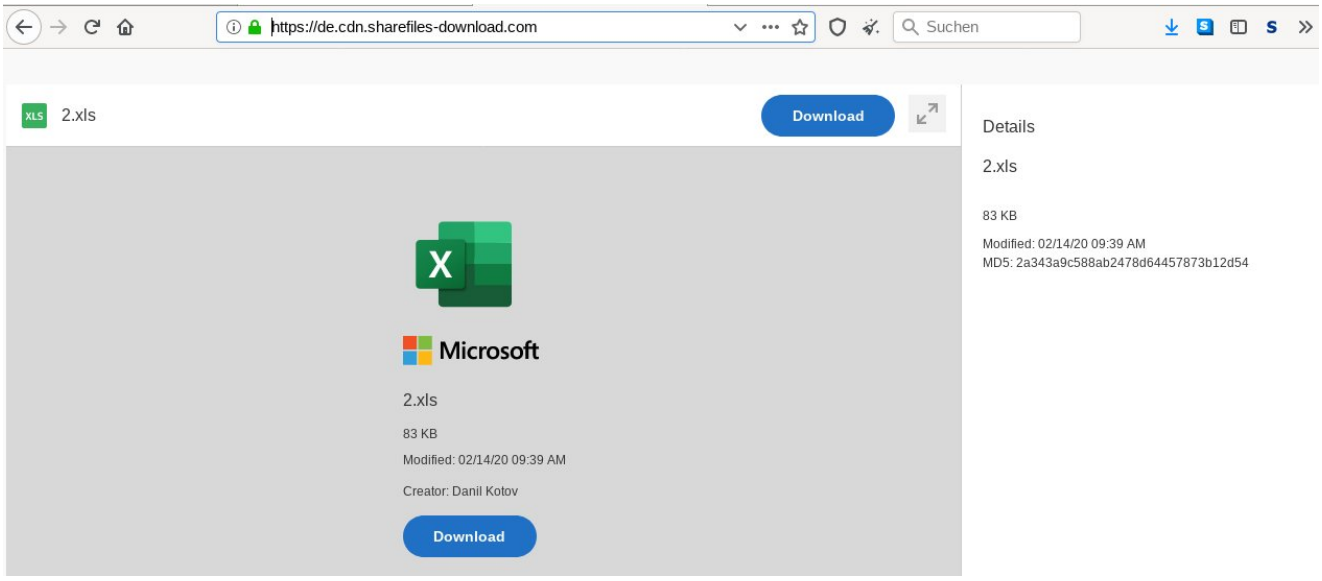


Figure 6 – Website used in Get2/SDBBot campaign, February 2020.

In the MirrorBlast campaign on 7 October 2021 (Figure 7), the website's design was almost identical to the one used in campaigns attributed to TA505. The reuse of the websites suggests that MirrorBlast and TA505 may be linked, or re-purposed by another threat actor with access to the website source code.

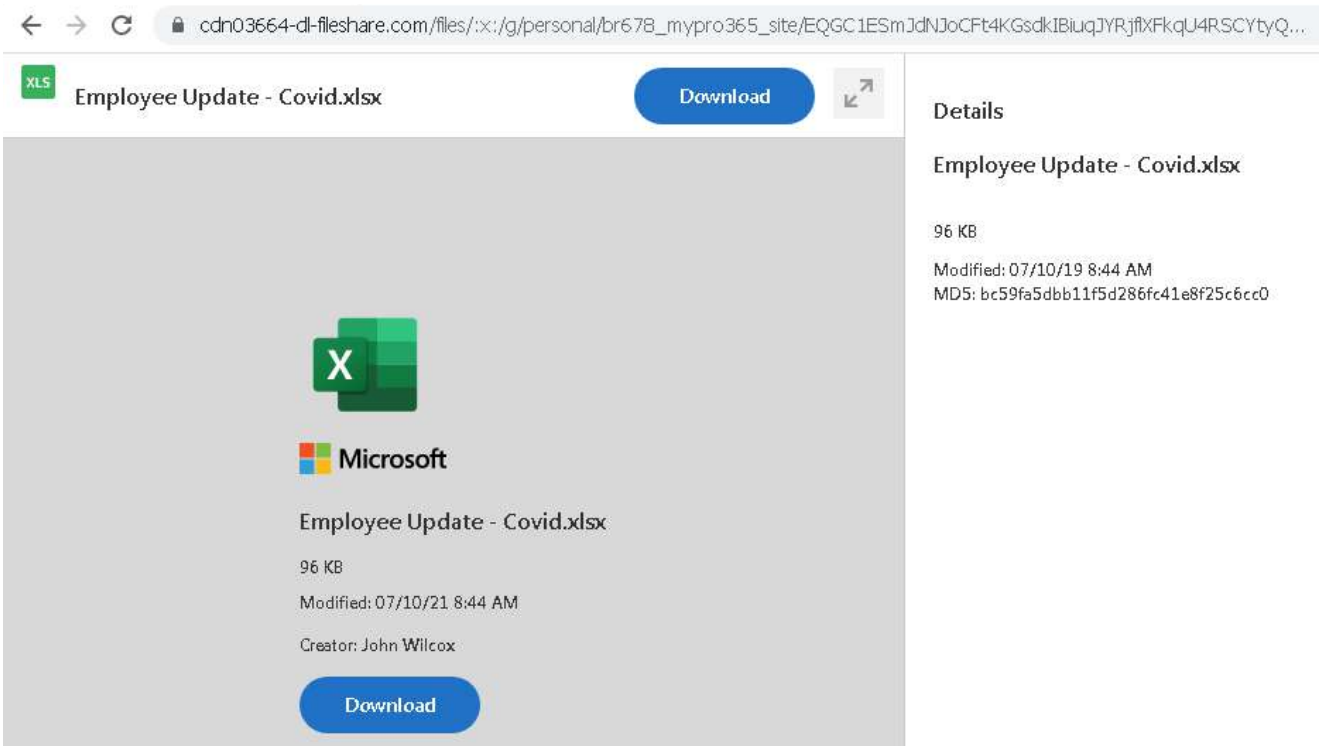


Figure 7 – Website used in MirrorBlast campaign, October 2021.

TA505 mostly used Excel documents to distribute Get2 and SDBBot. If you open the document, you will usually find an image designed to trick the user into activating Microsoft Office's macro functionality, which causes a malicious macro to run. These social engineering images varied in the Get2/SDBBot campaigns orchestrated by TA505.

Examining the images used in MirrorBlast lure documents reveals that they are almost identical to the TA505 documents (Figures 8 and 9).

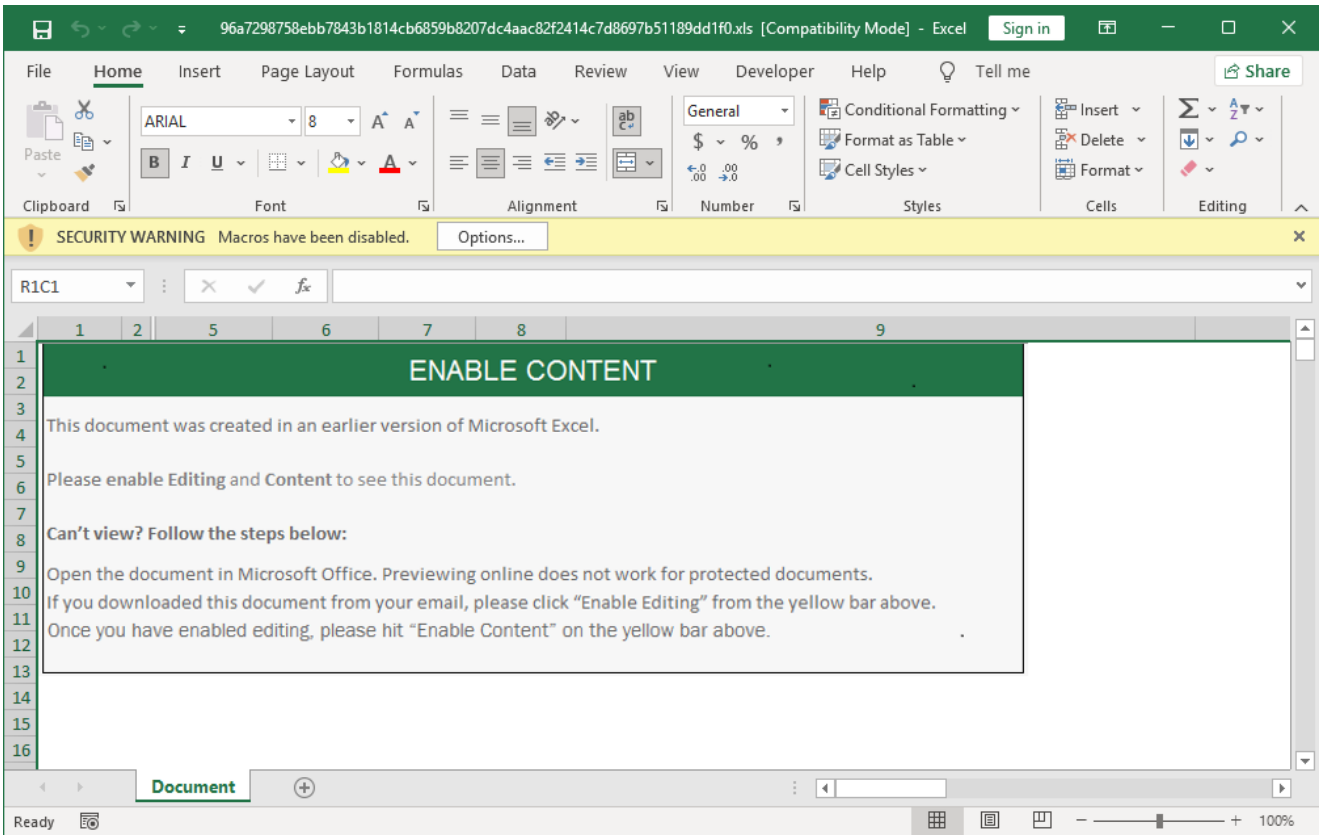


Figure 8 – Lure document in TA505 campaign, 19 August 2020.

The only major difference is that the MirrorBlast campaign targeted a German-speaking region, so the threat actor translated the text into German. However, if you look at the text closely, you will notice that the second to last sentence was not translated and is identical to the TA505 campaign. Such images and designs can be copied by other threat actors and used for their own purposes. For this reason, this similarity only weakly supports the view that MirrorBlast and TA505 are linked.

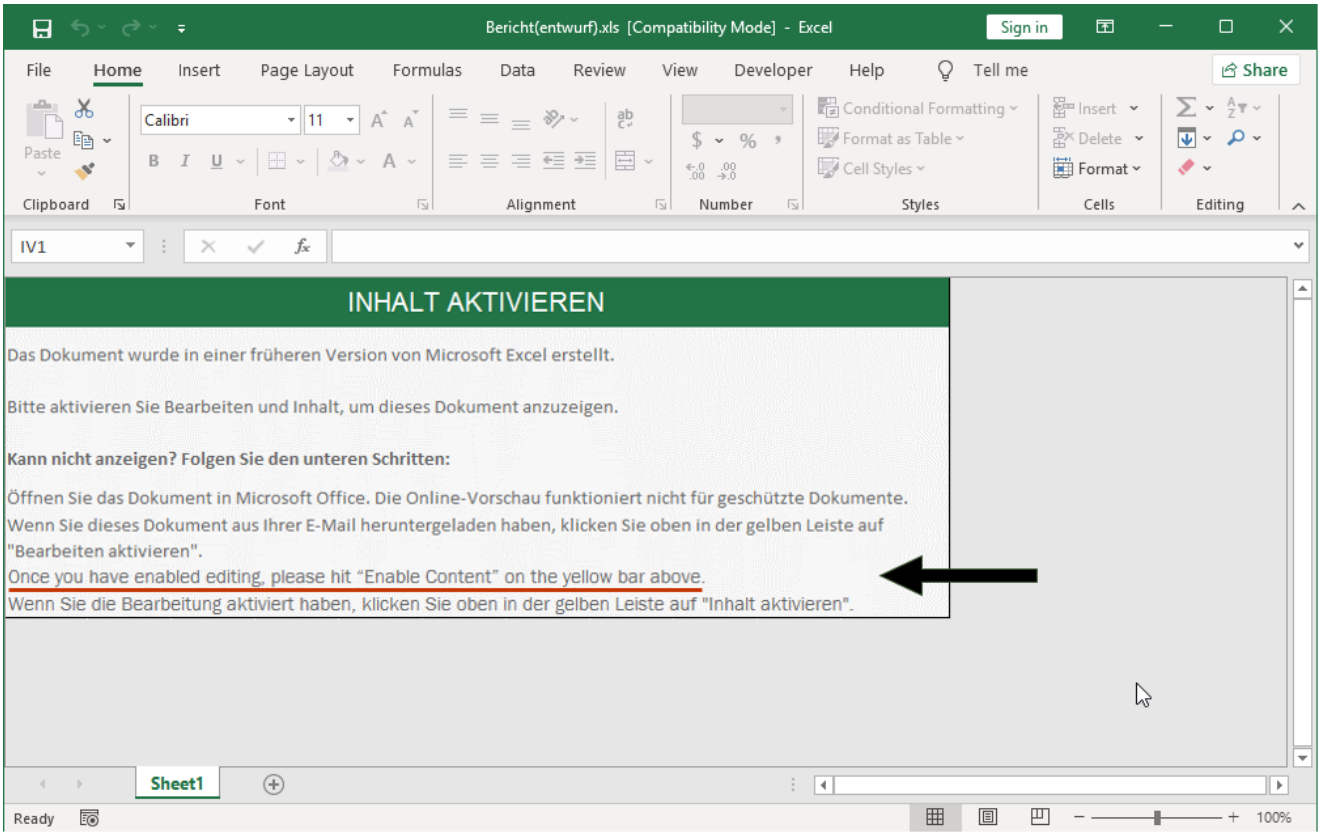


Figure 9 – Lure document in MirrorBlast campaign, 13 October 2021.

Similar Target Selection Mechanisms

The download websites used to distribute Get2, a loader used by TA505, were selective about which visitors to infect. Namely, they only offered the malicious Excel document to visitors with a Windows User-Agent. If a user with a different User-Agent finds their way to the website, they are redirected to Apple’s iOS website.

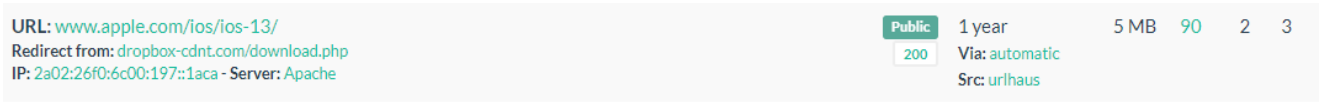


Figure 10 – Website redirect used in a TA505 campaign.

We found similar target selection behavior when looking at the MirrorBlast download websites. If you visit the website with a non-Windows User-Agent, you are also redirected to the Apple iOS website.

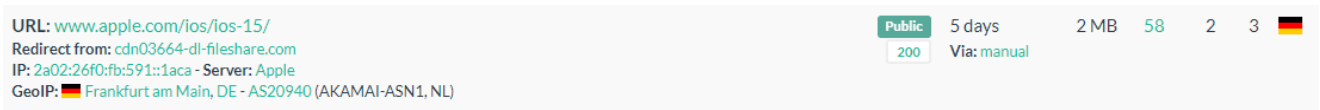


Figure 11 – Website redirect used in a MirrorBlast campaign.

This similar behavior is interesting, but also can be used to detect new TA505 and MirrorBlast domains. For example, urlscan.io, an online URL scanning service, has a search feature that network defenders can use to find TA505 and MirrorBlast URLs submitted to the service:

- *page.url:"*/ios/ios-13*"*
- *page.url:"*/ios/ios-15*"*

In the known Get2 campaigns of TA505, a short reconnaissance phase took place after the initial infection. The computer name, username, Windows version, and a list of active processes were collected and sent to the C2 via an HTTP POST request. The C2 responded with a cookie and URLs leading to the next malware stage depending on this information. This mechanism gives TA505 the ability to select which infected systems to deliver the next malware stage, thereby minimizing delivery to malware analysis systems and targets of little value.

MirrorBlast performs similar checks. In the KiXtart phase, which occurs after the Excel macro code executes, the malware sends various information about the client to a C2 server. This includes the domain name, computer name and username.

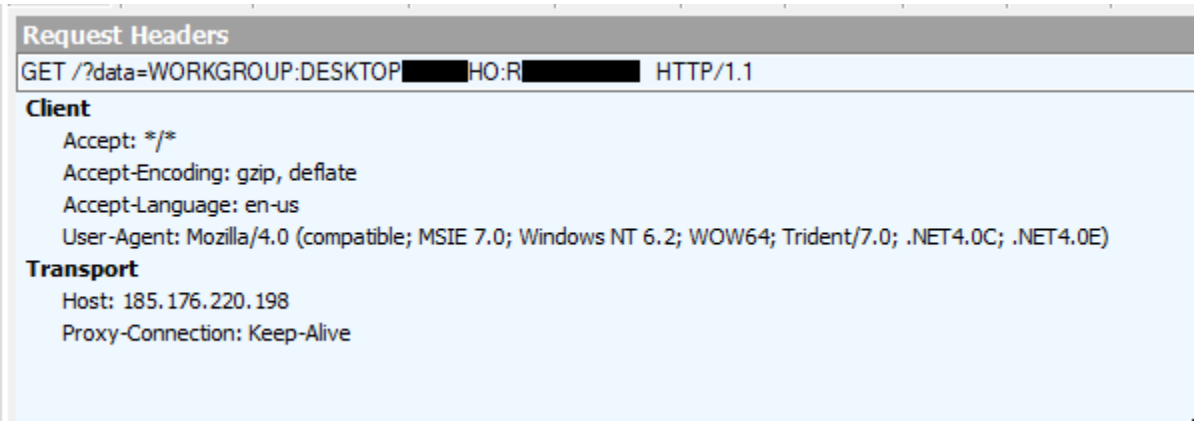


Figure 12 – System information sent to C2 in KiXtart phase.

If this information originates from a client of interest to the attacker, the next malware stage follows. In the Rebol phase, information about the client is again collected. The computer name, username and system architecture are transmitted to a C2 via an HTTP GET request.

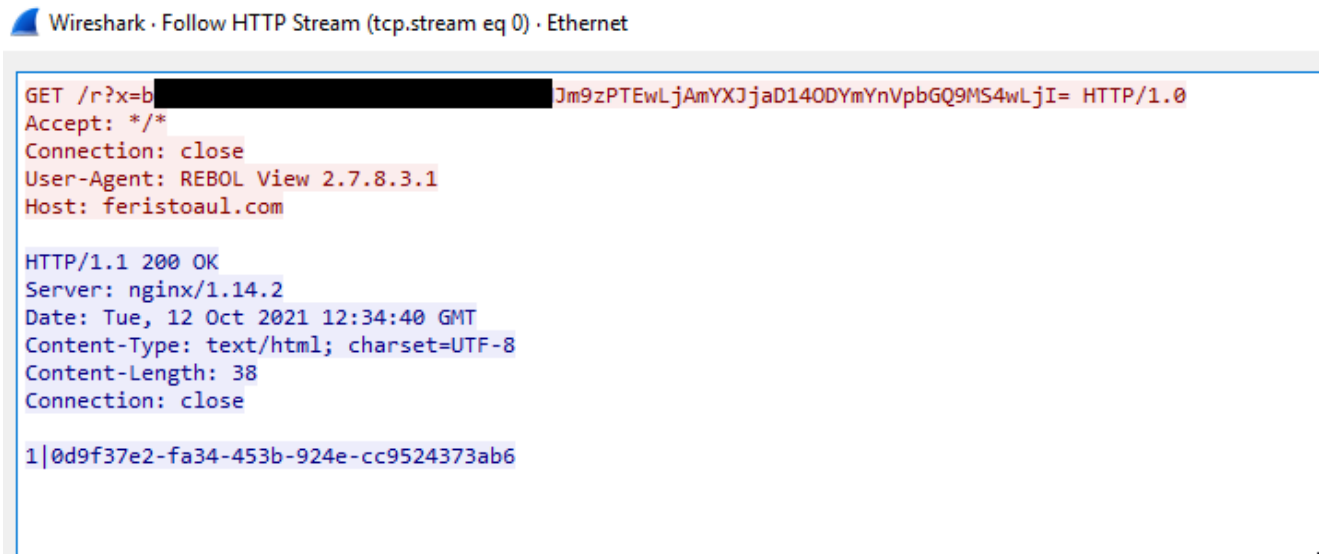


Figure 13 – Base64 encoded system information sent to C2 in Rebol phase, with a UUID returned.

In response, the C2 server returns a UUID. This UUID is encoded in Base64 and used as an argument in subsequent HTTP GET requests. This way, the C2 operator can select which systems they want to infect.

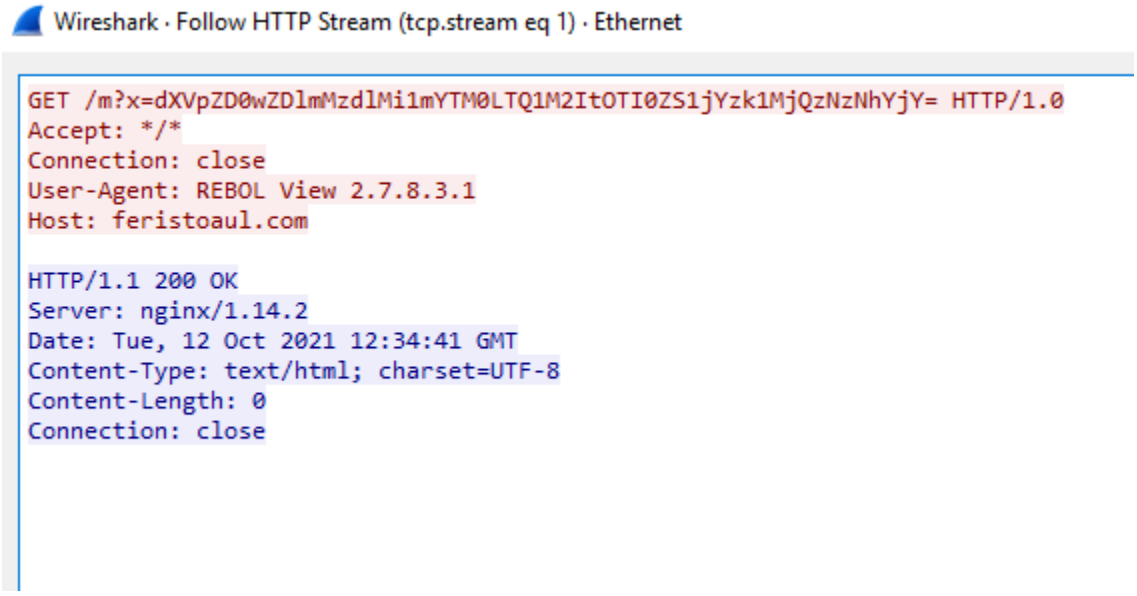


Figure 14 – Base64 encoded system information sent to C2 in Rebol phase, with no UUID returned.

Follow-up Malware

Another similarity between TA505 and MirrorBlast is the malware that is eventually delivered to an infected system. According to public reports, the follow-up malware of a MirrorBlast campaign is FlawedGrace (GraceWire). FlawedGrace is a remote access Trojan (RAT) that

was often used by the TA505 group. A report from ANSSI indicates the malware was used exclusively by TA505 in mid-2020. Assuming that FlawedGrace is only available to TA505, the appearance of FlawedGrace in MirrorBlast campaigns is strong evidence that MirrorBlast is closely linked to TA505. However, whether TA505's exclusive control over FlawedGrace has extended beyond mid-2020 is unclear.

Conclusion

This article compares the TTPs used in MirrorBlast and TA505's Get2/SDBBot campaigns. We focused on similar characteristics between the two. Whether TA505 is behind the MirrorBlast campaigns or another threat actor is responsible is not definitively clear based on these similarities, so we leave this for the reader to decide. Regardless of who is behind MirrorBlast, the campaign uses novel techniques (i.e. the KiXtart and Rebol phases) and has ramped up its activity in recent weeks. Therefore, we recommend organizations to implement prevention and detection measures to prevent infection with this malware. To accompany this article, we have published indicators of compromise (IOCs) of known MirrorBlast campaigns in the Appendix.

IOCs

Observed MirrorBlast Campaigns:
cdn03664-dl-fileshare[.]com
XLS: 2acdd04554feb1ef8b0307d5fb2c1bf7fd6a8e1157f9d3753119e64b30c16c30
KiXtart payload download: 185.225.19[.]246
MSI KiXtart: a403eae5b12b909f4075e855f58d1742308d5e0d3450e79b60162fa9fb7caad7
KiXtart C2: 185.176.220[.]198
Rebol payload download: 5.188.108[.]40
MSI Rebol: a69d27abd043cc676095f71300bf6b2368167536fcd4fe5342cf79a7e94fc2fe
Rebol C2: feristoaul[.]com
dzikic-my-sharepoint[.]com
XLS: 4648edc370e61a52c95d3f525391e0154406fd661d01d091f2d9dba9f8a485f2
KiXtart payload download: 185.10.68[.]235
MSI KiXtart: 2b108ec3e467ab6c3a9ad6a5545e8410e4185f8fee7a008d3d3a89a8caf86e75
KiXtart C2: 185.202.93[.]201
Rebol payload download: 185.225.19[.]156
MSI Robol: 0e6451e1f0eadb89390f4360e2a49a2ffb66e92e8b3ae75400095e75f4dd6abb
Rebol C2: fidufagios[.]com
dzikics-my-sharepoint[.]com
XLS: f4891094d6623dadbf84486b85a29b4bd0badf28ee100bc0e44c550715614e62
KiXtart payload download: 185.10.68[.]235
MSI KiXtart: ed7709cbbad9e164a45235be5270d6fb3492010ea945728a7d58f65f63434e58
KiXtart C2: 185.183.96[.]147
Rebol payload download: 192.36.27[.]92

MSI Robol: 0e6451e1f0eadb89390f4360e2a49a2ffb66e92e8b3ae75400095e75f4dd6abb
Rebol C2: fidufagios[.]com
cdn-8846-sharepoint-office[.]com
XLS: 28221d5ed7a6b37a4a0e5be77a9137378b1b6ca850c6327b77eae7a2b4437c96
KiXtart payload download: 155.138.205[.]35
KiXtart MSI: 83e4c90dc8bc1c53a4000bef83a355c4e36d2a1ba4a5d0982bc5b9b350278f1f
KiXtart C2: 45.79.239[.]23
cdnfilesdrop[.]com
cdn0341.us-dropbox[.]com
cdn9883.us-dropbox[.]com
XLS: 67af798c2d8e2a5d19fb304d60aca9c40cc23ae40d350ddef0c9a8ac95e94555
Rebol payload download: hxxp://23.19.58[.]52
Rebol MSI: eceb164a69e8f79bb08099fcdf2b75071c527b0107daebc0e7a88e246b4c7f13
Rebol C2: feristoaul[.]com

Potential follow-up malware:

hxxp://141.164.41[.]231/host64_sh.bin
hxxp://141.164.41[.]231/host32_pic.bin
hxxp://5.149.255[.]14/host64_sh.bin
hxxp://5.149.255[.]14/host32_pic.bin
hxxp://89.44.197[.]46/host64_sh.bin
hxxp://89.44.197[.]46/host32_pic.bin
hxxp://193.42.36[.]110/host64_sh.bin
hxxp://193.42.36[.]110/host32_pic.bin
host64_sh.bin: c1b4a0b9eadbf51e13343270b7ef85703b8a11ee736526f61193b821a72bef1f
host32_pic.bin:
aa42da6f08308796d2f1a61ea4aa79ac6054b2f57670e553d7fda481bd521737
C2: cdn-wfs-nspod[.]com

Tags

mirrorblast ta505