

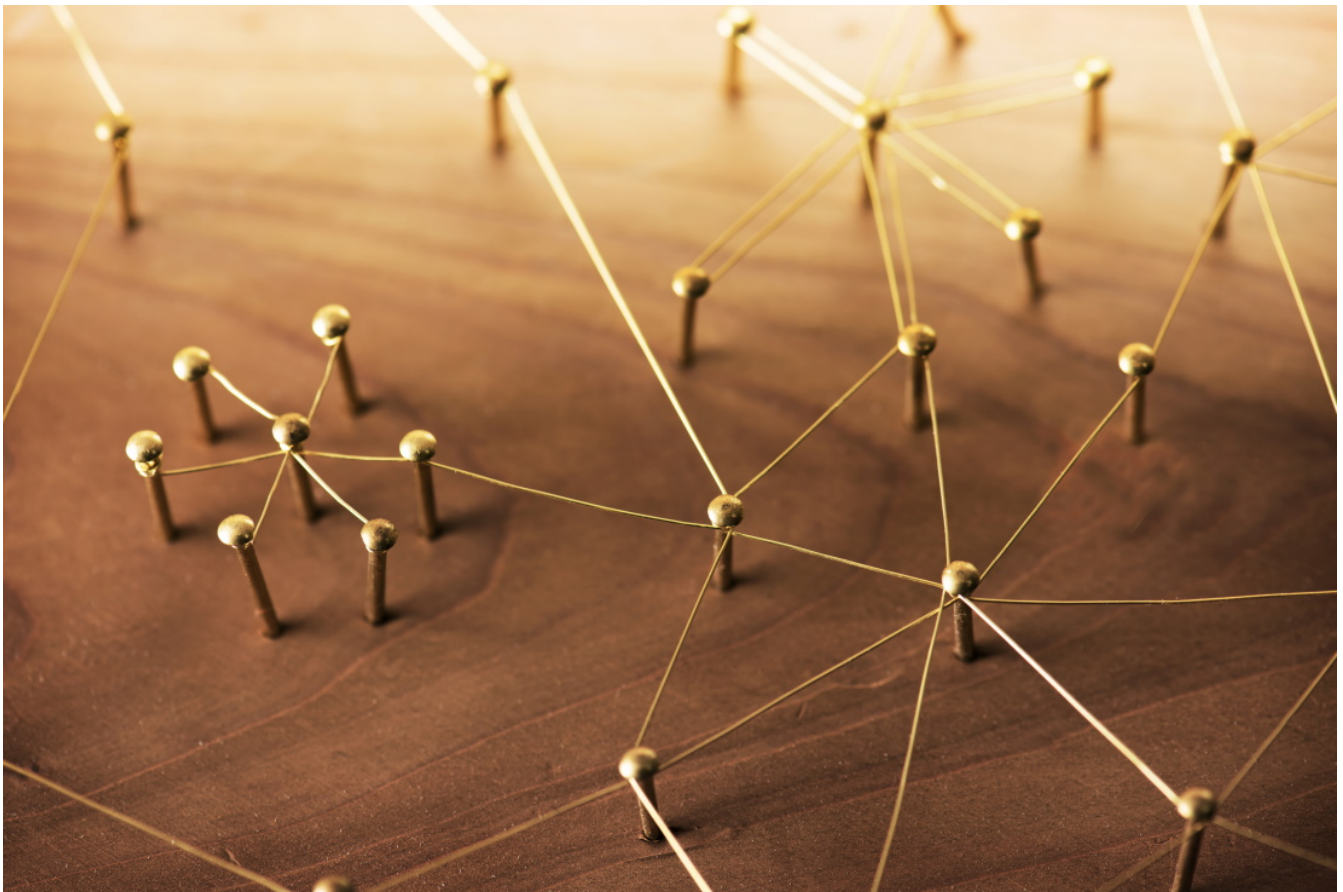
# Operation TA505: network infrastructure. Part 3.

 [ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/](https://ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/)

Positive Technologies

 **positive technologies**

Published on 24 May 2020



Network infrastructure analysis plays an important role in the study of malware distribution campaigns. Data on which IP addresses corresponded to a given domain name over time facilitate the identification of new malicious servers. In turn, retrospectively determining which domains were resolved to a given IP address provides new domains, for which the search procedure can be repeated, leading the process further. This information can be immensely helpful in establishing the geography of nodes, identifying "favorite" hosts and registrars, and determining which values an attacker characteristically enters into fields when registering domains.

Metainformation that appears useless at first glance may very well prove its worth after a period of a days, weeks, or months. In the course of malware analysis, sooner or later the question of attribution inevitably arises, and indirect identifiers such as network indicators can go a long way in determining which criminal group a certain tool belongs to.

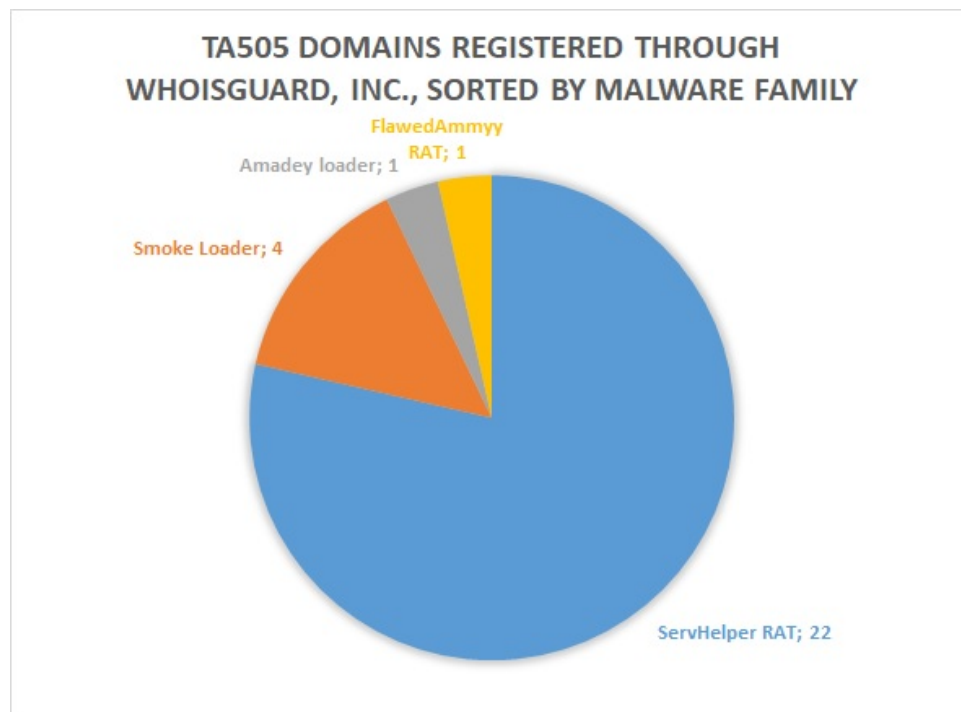
This article examines the most characteristic network infrastructure indicators of the TA505 group, as well as intersections between TA505 and another hacker group, Buhtrap.

## Domain name registrars

In total, we analyzed 372 domains belonging to TA505 and identified 22 organizations that facilitated the acquisition of these domains. The resources most frequently used were the following:

- WhoisGuard, Inc. — 28 domain names
- Eranet International Limited — 26 domain names

WhoisGuard, an organization based in Panama, offers the service of concealing domain owners' registration data from public access. This is not the first time we have seen their services used by hackers to establish anonymity and hinder investigations.



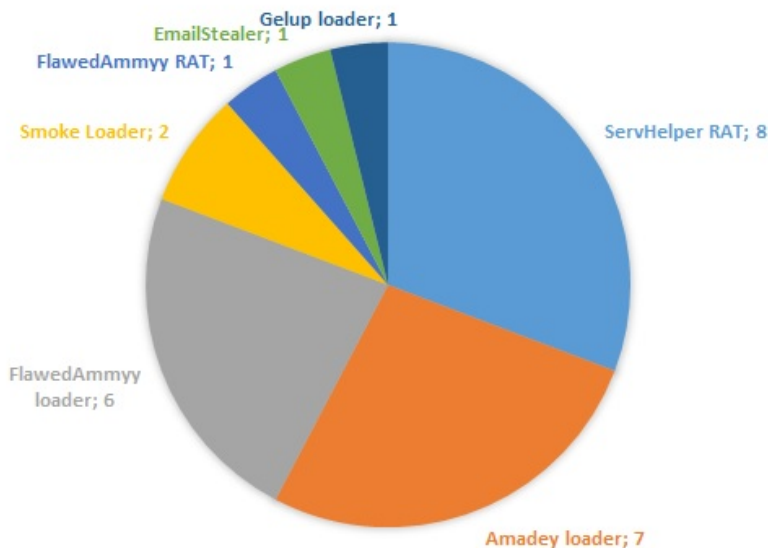
TA505 domains registered

through WhoisGuard, sorted by malware family

TA505 has utilized other, similar services, though to a lesser extent. These include PROTECTSERVICE LTD, Whois Privacy Protection Foundation, and Domains by Proxy LLC.

Eranet International Limited is one of the largest registrars in Hong Kong. It should be noted that members of TA505 tended to use dynamic DNS when registering domains with this provider. As a result, the IP addresses that their domain names were resolved to changed frequently, making them difficult to track.

## TA505 DOMAINS REGISTERED THROUGH ERANET INTERNATIONAL LIMITED, SORTED BY MALWARE FAMILY



TA505 domains

registered through Eranet International Limited, sorted by malware family

### Domain name registrants

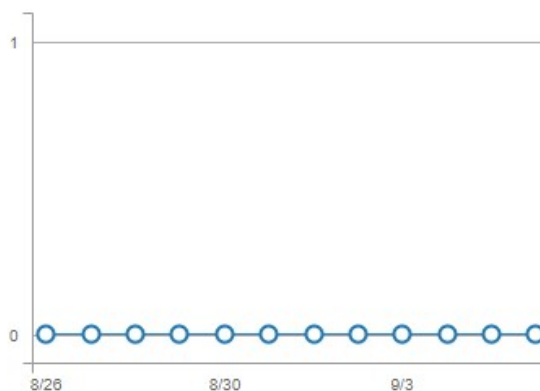
While investigating the WHOIS data of various domain names, we were able to obtain unique values for certain fields in a number of cases.

WHOIS data for TA505 domain names

Domain	WHOIS field	Value	Malware
kentona[.]su	Email	ctouma2@gmail.com	Smoke Loader/RMS RAT
koppepan[.]app	Email	nox1u9bruzgg@contactprivacy.email	FlawedAmmy loader
0141koppepan[.]com	Email	0141.koppe.pan@gmail.com	FlawedAmmy loader
elast[.]pw	City	hai dian hai dian	ServHelper RAT
Name	Lei Sun Lei		
Phone	+86.15810310076		
Email	std3199@163.com		
makosoft[.]jhu	Email	takagimeister@gmail.com	EmailStealer
bigpresense[.]top	Fax	+1.7246992079	EmailStealer
Email	armstrongdom@slimemail.com		
solsin[.]top	Organization	Brandon P. Thurman	FlawedAmmy loader

Domain	WHOIS field	Value	Malware
Fax	+1.3084575035		
Email	BrandonPThurman@grr.la		
newfolder2-service[.]space	State	smolenskaya oblast	Smoke Loader
Phone	+7.9385040686		
Email	ssserviceshop1@yandex.ru		
windows-several-update[.]com	Street	NO.1111 Chaoyang Road	FlawedAmmy loader
Name	Wiet Lee		
Phone	+86.86756381050		
Email	whois-protect@hotmail.com		
windows-update-02-en[.]com	Street	Shinararneri str. 43	FlawedAmmy loader
Name	Artak Gasparyan		
Phone	+374.37494527465		
test-service012505[.]com	Street	Mangilik yel, 52, 102	Smoke Loader
Name	Askar Dyussekeyev		
Phone	+7.71727172		
microsoftsyncservice[.]biz	Organization	zhuhaiyingxunkejiyouxiangongsi	Smoke Loader
office365onlinehome[.]com	Organization	Internet Invest, Ltd. dba Imena.ua	ServHelper RAT
Street	Gaidara, 50 st.		

Naturally, not all this information can be taken at face value. There are, however, certain values particularly worth noting. For instance, a search on the email address **ctouma2@gmail.com** leads to a [list](#) of additional domains registered to the same address. Another email address, **0141.koppe.pan@gmail.com**, is linked with a variety of resources—an account on [Github](#), [Steam](#), the Japanese hacker forum [Qiita](#) (with a link to a malicious domain in the profile), a [YouTube](#) channel, an account in Skype (live: 141.koppe.pan), and so forth.



**Koppe Pan**  
@0141KoppePan

Follow

【名称】0141KoppePan 【原材料名】Linux, Windows, Android, macOS, iOS 【添加物】Python, Go, Shell, HTML, CSS, JavaScript 【保存方法】高温多湿および直射日光を避け、涼しい場所に保管してください。

<https://0141koppepan.com>

- Following Tags 7
- Vim
  - nuxt.js
  - JavaScript
  - Vue.js
  - Python3

2 Items

0141KoppePan posted on Apr 21, 2018  
【4/25更新】CentOS7上でNGINX Unitを  
Python Python3 centos7 nginx-unii

0141KoppePan posted on Mar 10, 2019  
VPS(Vultr)と家のPCをVPN(WireGuard)で編  
VULTR kubernetes wireguard

Page on the

### Quiita hacker forum linked with suspicious domain registrant

We will refrain from delving into a deep analysis of these WHOIS data, as it lies outside the scope of this article. We will, however, note that hackers often utilize legitimate resources that have been compromised to host the first stage of their malware campaigns. The following domains are cases in point:

- greenthumbsup[.]jp
- fakers.co[.]jp
- nanepashemet[.]com
- nagomi-753[.]jp
- iluj[.]in

## Autonomous systems (AS)

For the sake of completeness, here are the top autonomous systems to which the IP addresses of C&C servers used by TA505 belong. Of course, a single autonomous system serves many hosts, both legitimate and non-legitimate, including various malware families of disparate origins. The following statistics should simply be viewed as an overview of the attacker's preferences. Taken with other data, they can be used for attribution.

Autonomous systems frequently used by TA505



```

mov     edx, ds:off_1002198C ; "52637245684563596857626D68547A73"
lea     eax, [esp+2F0h+var_258]
mov     ecx, ds:off_10021988 ; "2AAC28kdjQ0NCU8XuYmNhV3br5TveM5yiPXk8qk"...
push   eax ; int
push   edi ; Dst
push   edi ; char
call    fstr_decrypt ; compatexchange-cloudapp.net
mov     edx, ds:off_10021984 ; "7A5552576354456A6F5476666666C5775"
lea     eax, [esp+2FCh+var_2D4]
mov     ecx, ds:off_10021980 ; "HqJl0czvpNNyt192br3Fmw=="
add     esp, 14h
push   eax ; int
push   edi ; Dst
push   edi ; char
call    fstr_decrypt ; 80
mov     edx, ds:off_1002197C ; "59596F756969774F7974677961757164"
lea     eax, [esp+2F4h+var_2AC]
mov     ecx, ds:off_10021978 ; "m21aUDUCSFkplChefiUFNQ=="
add     esp, 0Ch
push   eax ; int
push   edi ; Dst
push   edi ; char
call    fstr_decrypt ; /help/index.php
mov     edx, ds:off_10021974 ; "646461677077727A4F707A6854546D77"
lea     eax, [esp+2F4h+var_290]
mov     ecx, ds:off_10021970 ; "jesUgVSnNjdQwC8cqPXGna8YcOV5dFTiqPohGKr"...

```

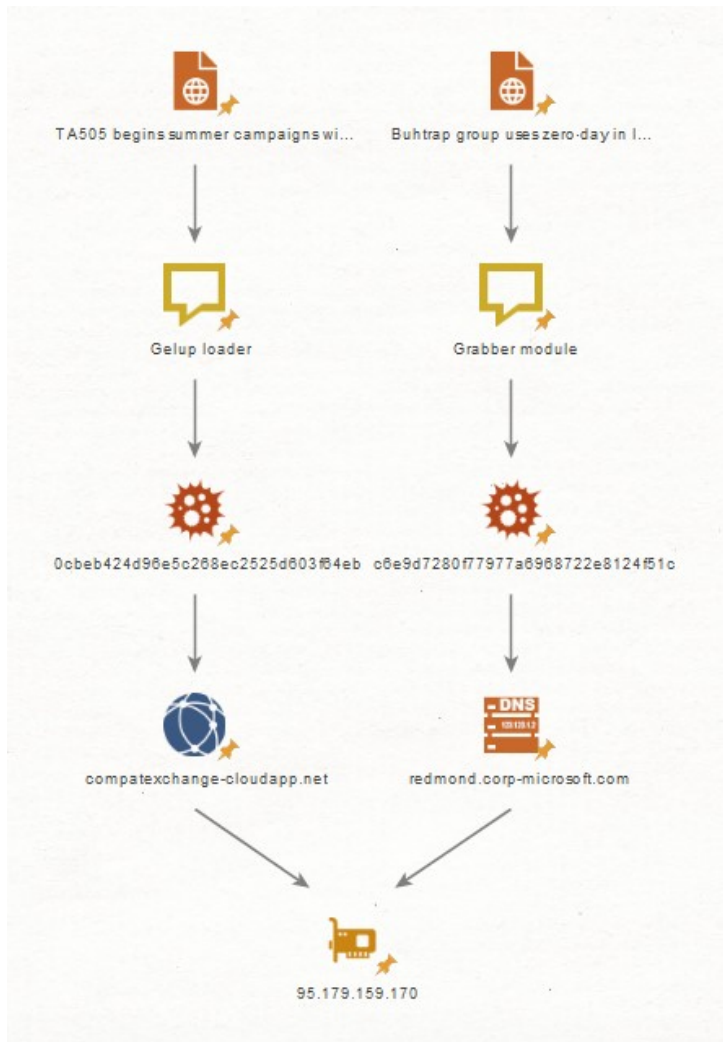
C&C server in Gelup from TA505,

after decryption

The [PaSiveTotal](#) resource shows us that this host has been resolved to the IP address 95[.]179.159.170 since June 8, 2019.

These two domains were registered with the same registrar (Tucows Domains Inc.) within two days of one another, and are resolved to the same IP address. Considering that both groups carried out attacks throughout June, it is reasonable to conclude that Buhtrap and TA505 used the same host as a C&C server.

It is also worth noting that the domain [compatexchange-cloudapp\[.\]net](#) was used not only in the downloader earlier discussed, but also in older versions of Buhtrap components.

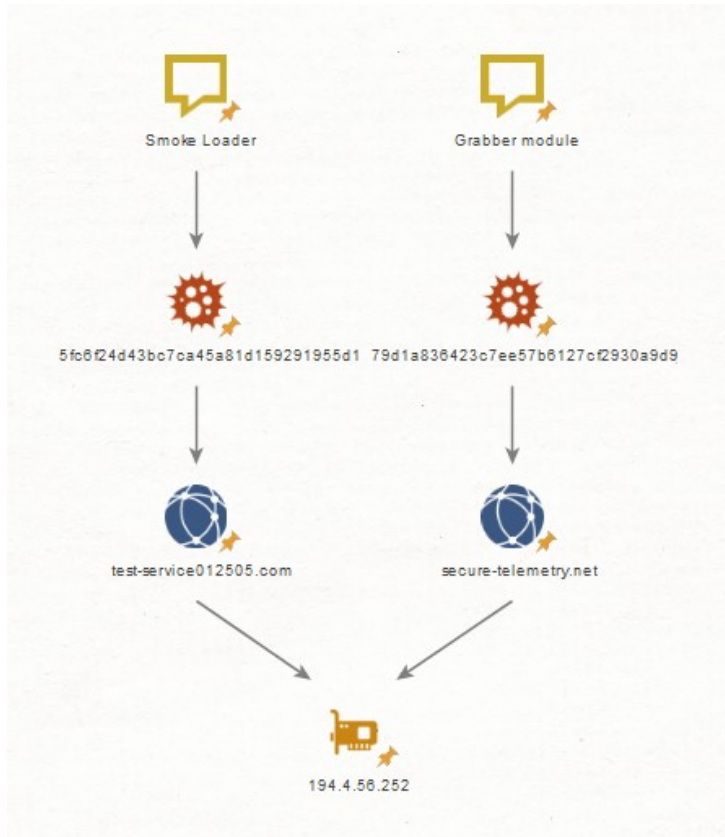


First intersection of TA505 and Buhtrap found in

network infrastructure

We later discovered another intersection between the two hacker groups. The domains of TA505's Smoke Loader and a second grabber from Buhtrap displayed a similar congruence: the domain test-service012505[.]com from Smoke Loader (MD5: 5fc6f24d43bc7ca45a81d159291955d1) and the domain secure-telemetry[.]net from the grabber (MD5: 79d1a836423c7ee57b6127cf2930a9d9) have been resolved to the IP address 194[.]4.56.252 since June 17th and 16th, 2019, respectively.





Second intersection of TA505 and Buhtrap found in

network infrastructure

## Conclusions

This article has examined the network infrastructure of the hacker group TA505. Starting with a look at their preferred domain name registrars and the hosts of their C&C servers, we unearthed interesting details in the client information provided by the group during domain registration. This could serve as a starting point for further investigations. We then discussed intersections that were discovered between the infrastructure of the TA505 and Buhtrap hacker groups. The incidence of shared servers between the two groups could have several explanations: the groups could have a bilateral agreement to share the servers, they could be managed and coordinated by a single entity, or they could both rent the servers from a third party (thereby economizing on expenditures). Our work investigating these groups will not end here. We will continue to monitor their activity and search for new information on their possible connections and collaboration.

**Authors:** Alexey Vishnyakov and Maxim Anfinogenov, Positive Technologies

## IOCs

TA505 C2:  
 0141koppepan[.]com  
 bigpresense[.]top  
 elast[.]pw  
 fakers.co[.]jpp  
 greenthumbsup[.]jpp  
 iluj[.]in  
 kentona[.]su  
 koppepan[.]app  
 makosoft[.]hu  
 microsoftsyncservice[.]biz  
 nagomi-753[.]jpp

nanepashemet[.]com  
newfolder2-service[.]space  
office365onlinehome[.]com  
solsin[.]top  
test-service012505[.]com  
windows-several-update[.]com  
windows-update-02-en[.]com  
c6e9d7280f77977a6968722e8124f51c — grabber module Buhtrap  
redmond.corp-microsoft[.]com — Grabber C&C  
0cbeb424d96e5c268ec2525d603f64eb — Gelup loader of TA505  
compatexchange-cloudapp[.]net — Gelup C&C  
95.179.159[.]170 — TA505 and Buhtrap shared host  
79d1a836423c7ee57b6127cf2930a9d9 — grabber module Buhtrap  
secure-telemetry[.]net — Grabber C&C  
5fc6f24d43bc7ca45a81d159291955d1 — Smoke Loader of TA505  
test-service012505[.]com — Smoke Loader C&C  
194[.]4.56.252 — TA505 and Buhtrap shared host