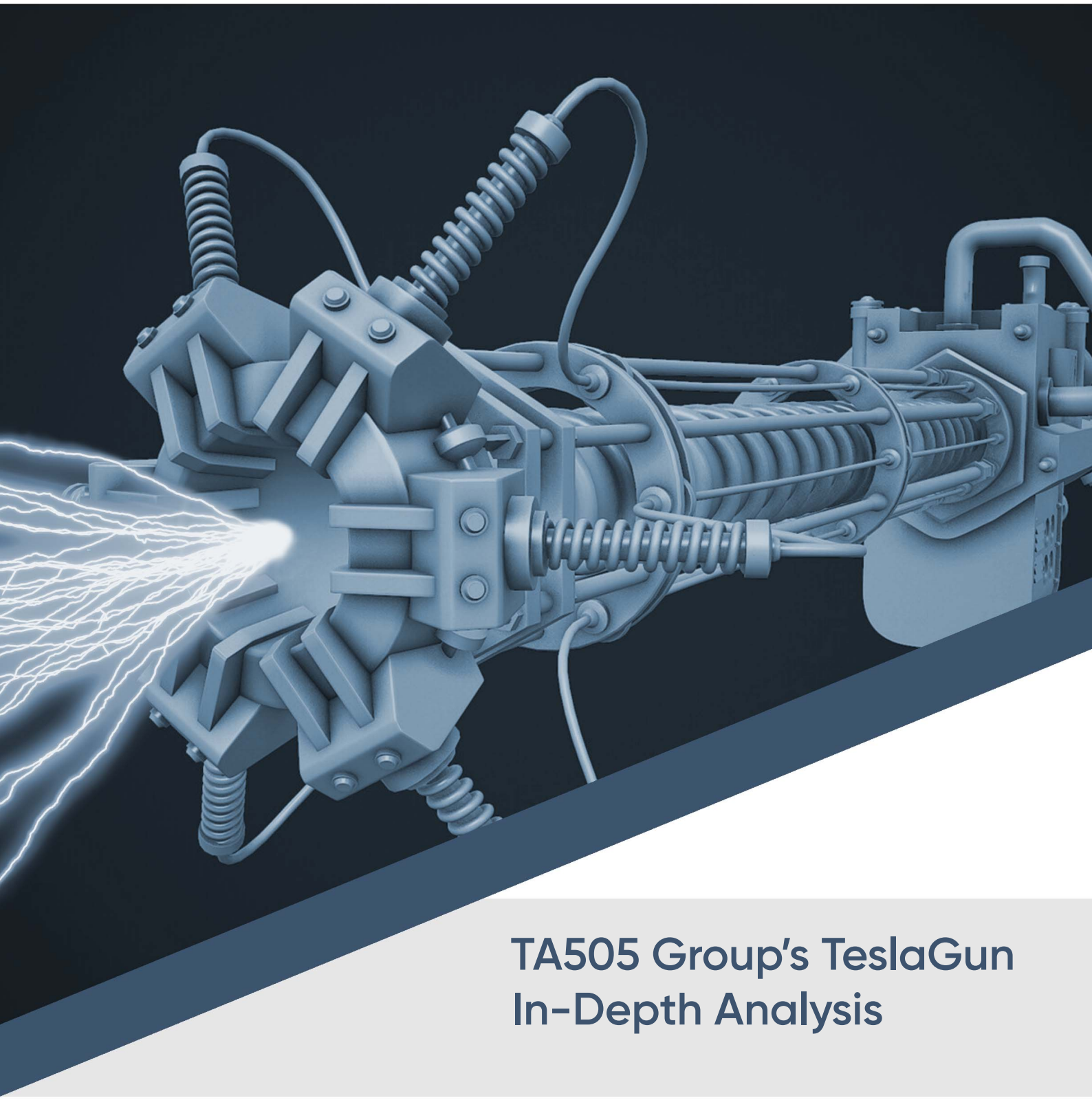
PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS



TA505 Group's TeslaGun In-Depth Analysis

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

Reference Number	CH-2022090501
Prepared By	PTI Team
Investigation Date	15.10.2021 - 01.01.2022
Initial Report Date	19.01.2022
Last Update	05.09.2022

1 Introduction

Backdoor attacks bypass standard authentication rules to access sensitive data and usually provide complete control of a victim's device with a persistent (but hidden) connection. These attacks can be challenging to detect because they circumvent many controls and policies designed to protect sensitive data against unauthorized access.

This report explores the command and control structure of one of the cybercrime industries' better-known backdoor malware variants. The TA505 threat group manages its **ServHelper** backdoor malware by using a software control panel called **TeslaGun**. TeslaGun name occurs on the top left of its control panels with a blue label and version number (can be seen in Figure 3).

TA505 is a financially motivated threat group that has been active since 2014. The group frequently changes its malware attack strategies in response to global cybercrime trends [5]. It opportunistically adopts new technologies in order to gain leverage over victims before the wider cybersecurity industry catches on.

This report provides insight into how TA505 enables and manages these attacks through its "TeslaGun" control panel. The PRODAFT Threat Intelligence (PTI) team identified the group's control panel and used it to glean insight into how the organization works.

This insight will help information security executives, legal professionals, and cybercrime insurers to understand the threat that TA505 poses to its victims. It will provide a clear foundation for resolving liability issues related to **ServHelper** attacks specifically, and backdoor attacks more generally.

Many reputable sources have already provided valuable sample analysis covering TA505's backdoor attack methods. This report focuses on new information; how the group's "TeslaGun" control panel enables the distribution of backdoor attacks, and what that can tell the cybersecurity community about TA505's motivations, strategies, and internal organizing principles.

This report holds valuable, previously unreported analysis of **ServHelper** campaigns and samples. Similarly, it contains findings from the group's C&C server, including infection dates, targeted countries, executed commands, and other valuable information regarding the group's techniques and tactics.

2 Executive Summary

2.1 Overview

The group has carried out mass phishing campaigns and targeted campaigns on at least **8160 targets**, largely focusing on finance sector companies and individuals. According to unearthed **TeslaGun** victim data, TA505 mostly targeted **the U.S**, which is home to **3667** of the group's victims (as shown in Figure 1).

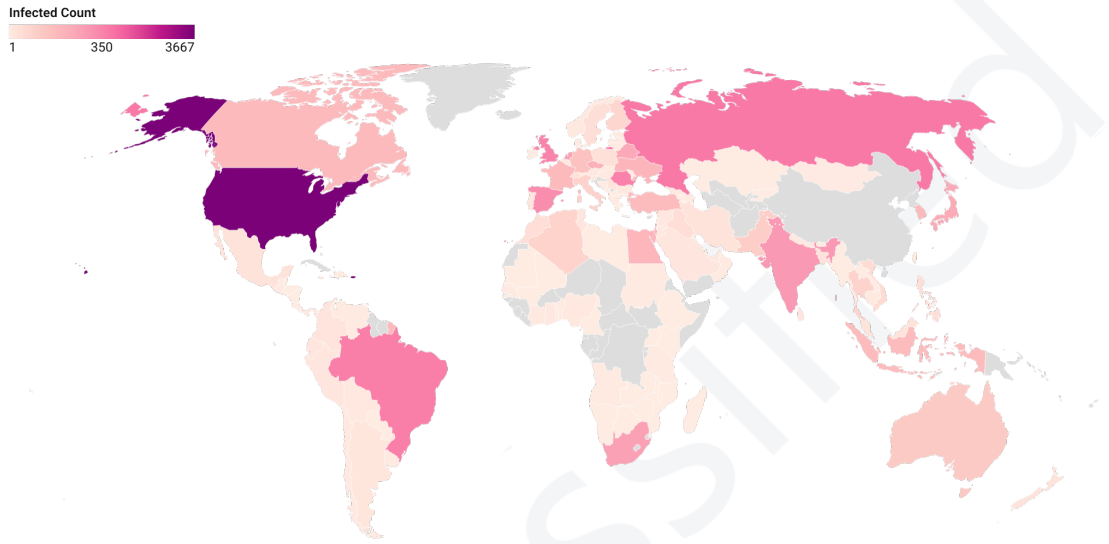


Figure 1. **Victim distribution by country.**

The group makes its priorities clear in a footnote located inside the **TeslaGun** panel, which says **"Huawey Coproration with love to USA"**, as shown in Figure 2 (The typo exists in the original text).

```
<center><a onClick="if (!confirm('Delete all?')) return false;" class="button is-danger" href="/pat924/askjnhvu.php?flushall=1">CLEAR ALL ENTITIES</a>
<br ><br >
provided from Huawey Coproration with love for USA
</center>
```

Figure 2. **Footnote of TeslaGun panel.**

2.2 Characteristics of the TA505 Group

Financial Motivation : The PTI team observed that the main dashboard of the TeslaGun panel includes comments attached to victim records. These records show victim device data such as **CPU**, **GPU**, **RAM size** and **internet connection speed**.

This information shows that "ServHelper" users are actively profiling their victims, and TA505 members may use this data to decide which victims' devices are suitable for crypto-mining.[4] On the other hand, according to victim comments, it is clear that TA505 is actively looking for online banking or retail users, including crypto-wallets and e-commerce accounts.

Targeting Financial Sector : According to the PTI Team victim analysis, most TA505 victims operate in the financial sector. However, it is readily apparent that TA505 opportunistically targets individuals and organizations in non-related sectors as well. The group dedicates resources to maintaining backdoor connections and actively tries to sell those connections to other cybercriminals4.

Malware Toolkit : According to the third-party technical analysis and samples available on public threat platforms, TA505 uses various droppers as well as delivery techniques for their backdoor malware attacks [2][4].

Targeted Countries : While the United States is by far the most frequently targeted region, with 3667 attacks recorded, TA505's next most common targets include Russia (647), Brazil (483), Romania (444), and the United Kingdom (359).

Fraudulent Activities : Although "ServHelper" does not need interaction or manual configuration, TA505 members often interact directly with victim devices through the Remote Desktop Protocol (RDP) with multiple sessions. The PTI team detected TA505 threat actors downloading and installing custom tools like (**sep12.exe**) via patched RDP sessions to carry out fraudulent activities.

Multiple Campaigns : A single instance of the "TeslaGun" control panel contains multiple campaign records representing different delivery methods and attack data. Newer versions of the malware encode these different campaigns as campaign IDs. We observed a significant number of different victim profiles and campaigns during our investigation. Other researchers analyzing the group's malware samples also concluded that TA505 operates multiple attack vectors, apparently and simultaneously [6].

3 Technical Analysis

This section analyzes the TA505 group's C&C infrastructure and the technology being used for RDP/VNC connections.

3.1 ServHelper

Although the **ServHelper** code base gets changed rapidly, one aspect of the software stands out, its backdoor account is named **WgaUtilAcc** and it can be found on user registries under **.../Winlogon/SpecialAccounts/UserList** [1]. The following table shows how this backdoor is being created in step-by-step format :

Command	Description
net user WgaUtilAcc <Password>	Creates WgaUtilAcc
net LOCALGROUP "Administrators" WgaUtilAcc /ADD	Adds backdoor user to Administrator group
net LOCALGROUP "Remote Desktop Users" WgaUtilAcc /ADD	Adds backdoor account to RDP group
net LOCALGROUP "Remote Desktop Users" %USERNAME% /ADD	Adds current account to RDP group
wmic path win32_VideoController get name	Gets GPU Name
wmic CPU get NAME	Gets CPU Name
powershell -ep bypass -NoProfile -outputformat text -nologo -noninteractive -enc %Trimmed...%	Execute connection speed testing script.

Once the PTI performed detailed analysis on one of TA505's TeslaGun panels, it could easily profile how ServHelper communicates with its C&C infrastructure. These profiles enabled the team to analyze samples on other sandbox and open threat exchange platforms, resulting in panels & IPs similar to those TA505 manages.

This does not mean that this report exhaustively covers all TA505 domains and IPs. The group may be operating additional domains through domain generation algorithms (DGAs) and proxy servers as well.

For example the domain, which is dkaknvizisic.xyz, has not been flagged in VirusTotal (at the of the investigation) as malicious for security. This domain occurs to be a brand new CC TeslaGun panel associated with 37 victims at the moment of our investigation. We have found data corresponding to these victims tagged with the sep27 campaign code.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing global fight against high-end threat actors and APTs such as TA505.

3.2 Infrastructure

The actors regularly migrate their proxy servers to new servers in the same datacenter to attain a low detection rate. During our investigation, we observed several TeslaGun management panels predominantly residing in MivoCloud SRL, Moldova, as show in Table 1. In this report, we did not include their new toolkit developed at the end of 2021 and its infrastructure for simplicity.

IP Address	Country	AS Name	First Seen
5.181.156.4	Moldova	MivoCloud SRL	07.05.2020
206.188.197.221	Netherlands	BL Networks NL	02.07.2021
185.163.47.171	Moldova	MivoCloud SRL	05.07.2021
185.163.47.210	Moldova	MivoCloud SRL	10.07.2021
194.180.174.56	Moldova	MivoCloud SRL	13.07.2021
94.158.245.77	Moldova	MivoCloud SRL	16.07.2021
5.181.156.142	Moldova	MivoCloud SRL	06.07.2021
94.158.245.113	Moldova	MivoCloud SRL	18.07.2021
94.158.245.172	Moldova	MivoCloud SRL	18.07.2021
5.181.156.64	Moldova	MivoCloud SRL	19.07.2021
206.188.197.203	Netherlands	BL Networks NL	19.07.2021
194.180.174.20	Moldova	MivoCloud SRL	20.07.2021
185.163.45.240	Moldova	MivoCloud SRL	24.07.2021
5.181.156.15	Moldova	MivoCloud SRL	26.07.2021
94.158.245.73	Moldova	MivoCloud SRL	11.08.2021
185.163.45.186	Moldova	MivoCloud SRL	11.08.2021
185.163.45.56	Moldova	MivoCloud SRL	12.08.2021
185.163.45.248	Moldova	MivoCloud SRL	24.09.2021
94.158.245.180	Moldova	MivoCloud SRL	05.10.2021
194.180.174.105	Moldova	MivoCloud SRL	15.11.2021

Table 1. TeslaGun's management infrastructure.

3.3 Command & Control Servers

The TeslaGun panel has a pragmatic, minimalist design. The main dashboard only contains infected victim data, a generic comment section for each victim, and several options for filtering victim records.

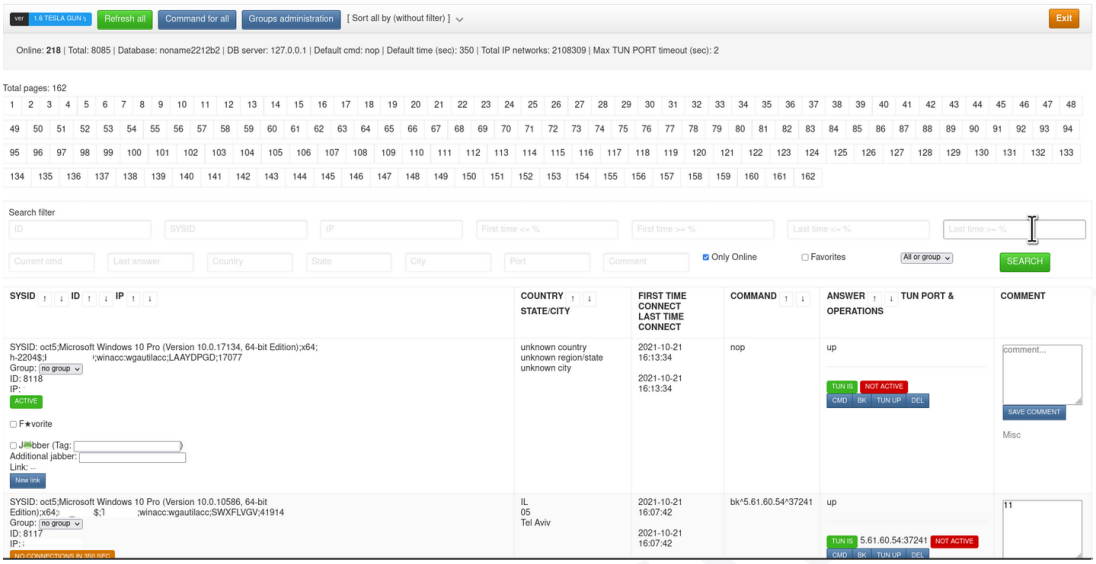


Figure 3. Dashboard of the TeslaGun management panel.

The panel's filtering options offer a great deal of information about TA505's workflow and commercial strategy. **Sell** and **Sell 2** groups were set for some victims. These victims' RDP connections were temporarily disabled through the panel.

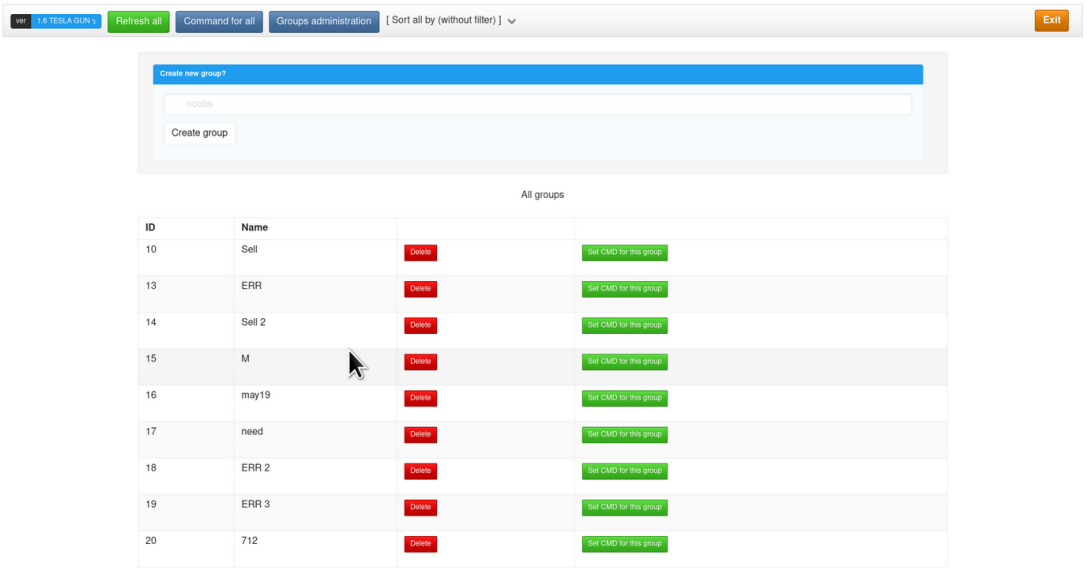


Figure 4. Victim groups.

This probably means that TA505 can not immediately earn a profit from exploiting those particular victims. Instead of letting them go, the group has tagged those victim's RDP connections for the resale to other cybercriminals.

The **ERR** group refers to those victims who have a **slow connection**. If the victim's connection is too slow, TA505's **RDP** connection will not work properly, and the group in this case loses the ability to communicate with ServHelper effectively.

TeslaGun panels do not provide individual victim detail pages. Instead, victim tables show data in a series of columns :

- SYSID/ID/IP
- Country/State/City
- First Time Connected/Last Time Connected
- Command
- Answer Operations/Tun Port/Operations
- Comments

The SYSID column refers to multiple aspects of the backdoor attack on a victim's device, as explained in Binary Defence's comprehensive blog[1]. This column shows the following data :

```
{Campaign Code};
{OS Name};
{Architecture};
{Computer Name};
{Local Account Name};
{Backdoor Account:WgaUtilAcc};
{Backdoor Account's Password}
```

The Cisco Talos's Intelligence Group [4] has already identified how these data relate to ServHelper's command list and functionalities. Panel users can send these commands to victim's devices through TeslaGun panels.

Moreover, TeslaGun has a functionality that allows attackers to send one command to all victim devices in one step, or to configure a default command that runs when a new victim device is added to the panel.

Figure 5 shows how running a command or changing the task for a specific victim works in the **TeslaGun** panel.

Figure 5. Sending command to victim device.

3.4 Post Infection

During this investigation, the PTI team discovered TA505 users executing RDP connections using tunnels. Other technical reports[4] also note this kind of activity, but do not mention where these tunneled connections are going.

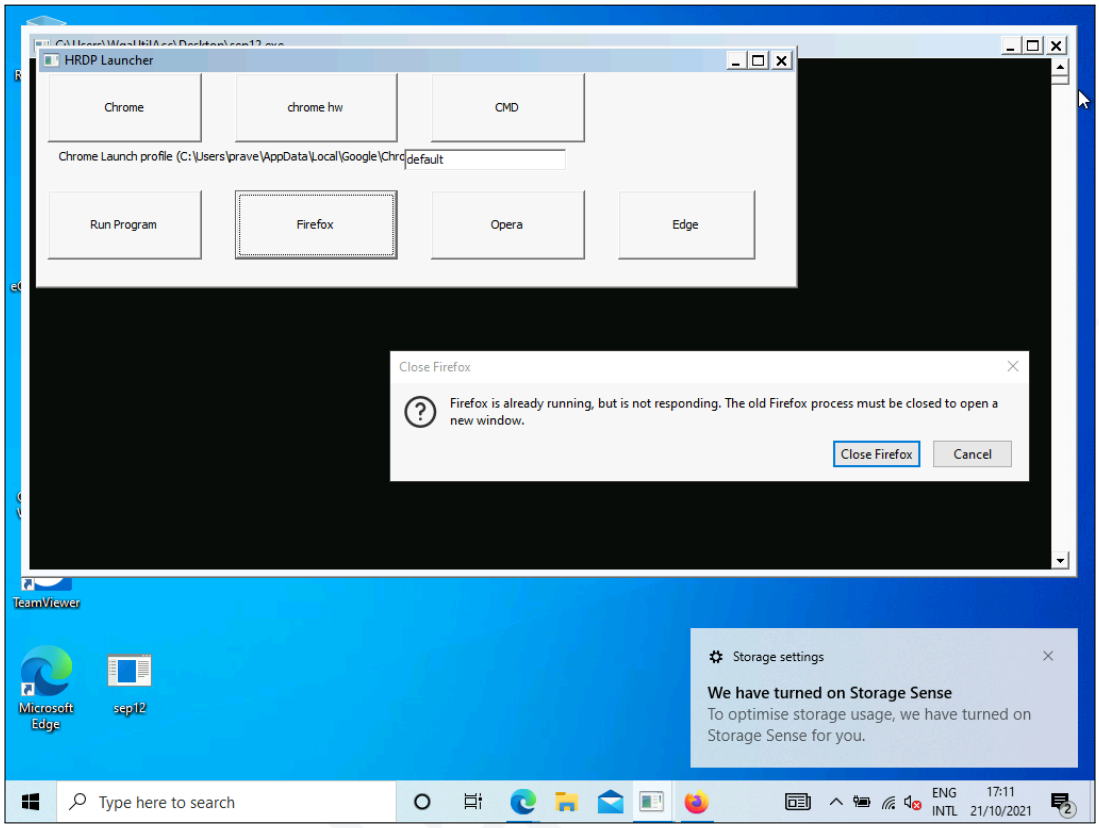


Figure 6. TA505 Member is installing sep12.exe into victim device.

This tool 6.2 lets attackers launch multiple hidden RDP instances. After infecting a victim, TA505 members connect to the victim via RDP upon infection to use these remote connections simultaneously.

Although, the samples communicate to panel domains, threat actors connect to their victim's RDP via tunnels. This command is called **"bk"** in the C&C panel. Threat actors can send the **"bk"** command to establish RDP tunnels, then connect to the victim's RDP through a selected port on a proxy server. These IPs are not flagged as malicious on public lists, which means TA505 can often bypass signature-based detection solutions.

Table 2 shows an IP list that corresponds to TeslaGun Panel's RDP/VNC proxy servers.

IP Address	Country	AS Name
5.61.60.5	United Kingdim	M247 LTD
23.227.194.15	United States	HVC-AS
37.1.201.136	Netherlands	Scalaxy B.V.

Table 2. RDP/VNC proxy servers found in accessed panels.

3.5 De-Anonymization

The PTI Team observed that threat actors would publish comments announcing when victim connections are sold. Table 3 shows all nicknames mentioned in these comments. Unfortunately, the comments do not provide enough context to determine what roles these users actually play in the marketing and sale of victim connections. These nicknames may represent buyers, sellers, or other kinds of transaction facilitators.

Cocayeene
Tr0nstr
DonBillisario
Bugerman
ZeNoN|Zen0n
Kadabr
Wolf158$
Maison
Benjamin
Gucci G
Ivan
Loc Dog
Andre
Tega
Topol
Gangster
Pes Barbos
Павел Ивлев|Pavel Ivlev
Bipbip
KP
roipaint

Table 3. Nicknames that are mentioned in comments.

4 Statistics & Observations

This section covers some of the important insights surrounding TA505's impact on different countries and victims. Here, we present our findings from the C&C server, which match the TA505 group's actions with the known timelines of several TA505 campaigns.

The PTI team's analysis shows that each C&C instance has a separate victim database. Victim record IDs as a result are not unique. TA505 uniquely identifies victims across databases by using their **SYSID**.

There is evidence that victims can be transferred across panels and instances. For example, in one panel located on **dfsrakizimoy34ggf.xyz**, the oldest victim was logged on **2020-07-15**, through a campaign tagged as **jul11**. However, according to Whois information for that domain, entry was updated at **2021-09-26 17:16:39.0Z**. Alternatively, the date of this domain was first seen is **2020-03-27 08:50** and the resolved IP was **5.181.156.5**. This IP is different, unlike the IP of the latest entry. This situation indicates that the victims must have been transferred from another instance. The PTI Team also detected that one single domain may include more than one panel, and these panels have different databases.

Unearthed information indicates that campaigns' samples are not only for single time use. For example, for **dec4** and **dec27**; the campaigns' oldest victims were first logged on **"2020-12-11"** and **"2021-01-03"** respectively. However, the **dec4** campaign's malware did not stop spreading after **dec27** was launched. One of **dec4's** victims was first logged on **"2021-01-13"**, right after the start of the **dec27** campaign. Much later, this iteration started to show up again in **August 2021**, and has been extended to **September 2021**.

This clearly shows that **TeslaGun** panels are not exclusively organized according to campaigns or versions. This makes it difficult to capture and define the overall structure of TA505 as an organization. The group may have additional activities outside the context of what the PTI team found during its investigation. Figure 8 represents the all versions of what the PTI team could gather from the TeslaGun panels investigateion.

4.1 Infection Rates

The graph 7 illustrates the amount of victims infected by the threat actors.

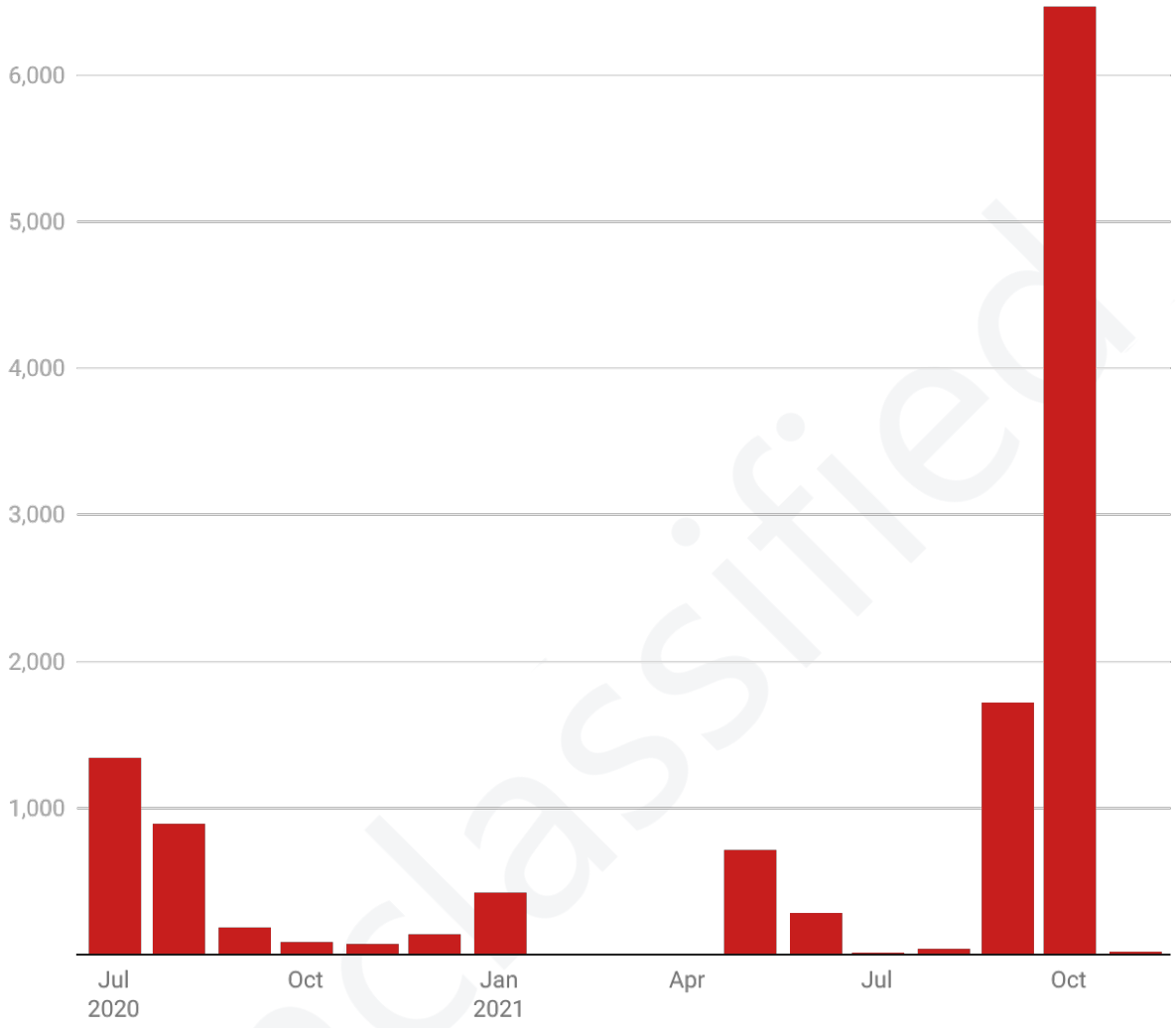


Figure 7. Victim infection count by date.

oct5 is the variation with the highest victim count (**6340**). According to the first victims logged in that campaign, **oct5** began attacking victims on **2021-10-06**, which indicates why the name **oct5** was chosen. This variation ran for a short time, closing on **2021-10-21**, indicating how disruptive and virulent it was compared to other campaigns. The graph 8 shows victim counts organized by campaign code.

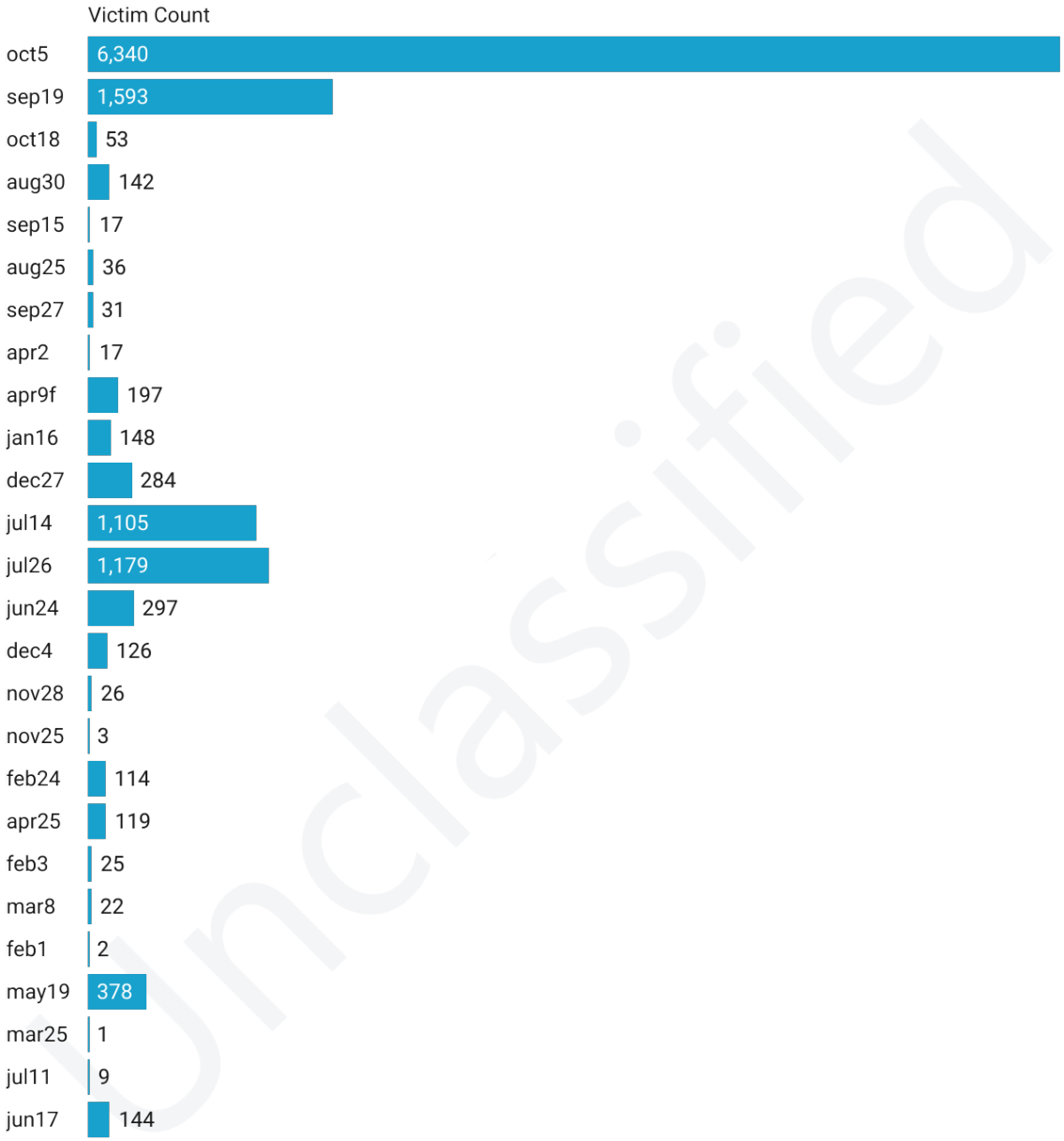


Figure 8. Victim infection count by campaign code.

4.2 Affected Countries and Sectors

The US is by far the most frequently targeted region with 3667 attacks recorded. TA505 has explicitly shown its preference for US victims with its "Huawey" footnote. This, alongside a notable preference for Chinese top-level domains, might be designed to implicate China in TA505's attacks.

However, it is possible that these signs are merely red herrings designed to throw threat intelligence operatives off-track. The general consensus of the cybersecurity community is that TA505 is probably located somewhere in Eastern Europe, and is motivated by direct financial gain rather than national politics. The group does not appear to exclude specific nationalities or languages the way some other cybercrime groups do. TA505 victims can be anyone from anywhere.

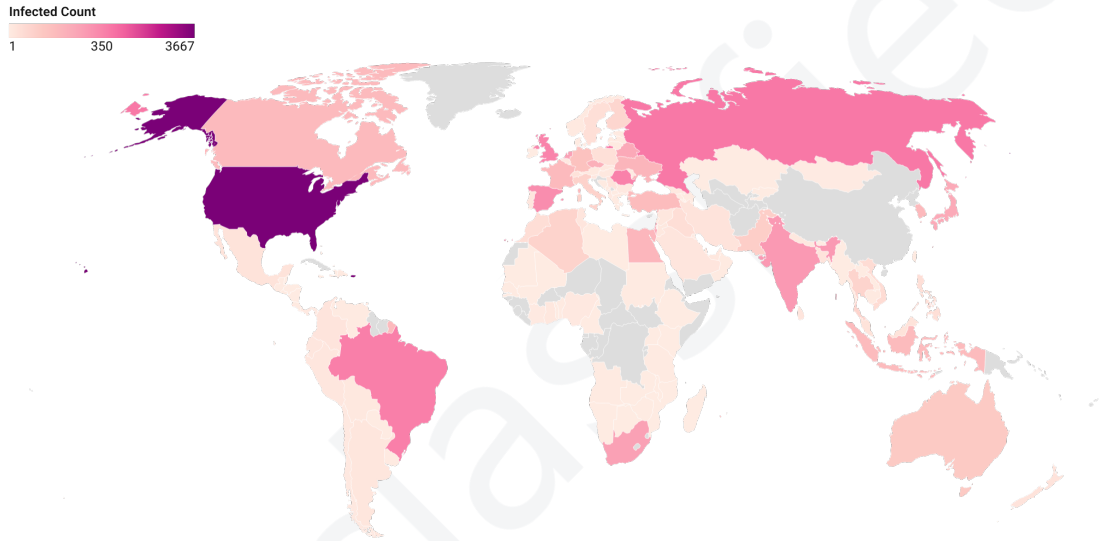


Figure 9. **Infected victims by country.**

It is plain to see that Romania is the most frequently targeted country in the European Union. Spain has also faced more attacks than most other EU countries. Russia and the United Kingdom are outside the EU but in close geographical proximity, and have similarly high numbers of victims. Figure 10 illustrates the number of victims from Europe, organized by country.

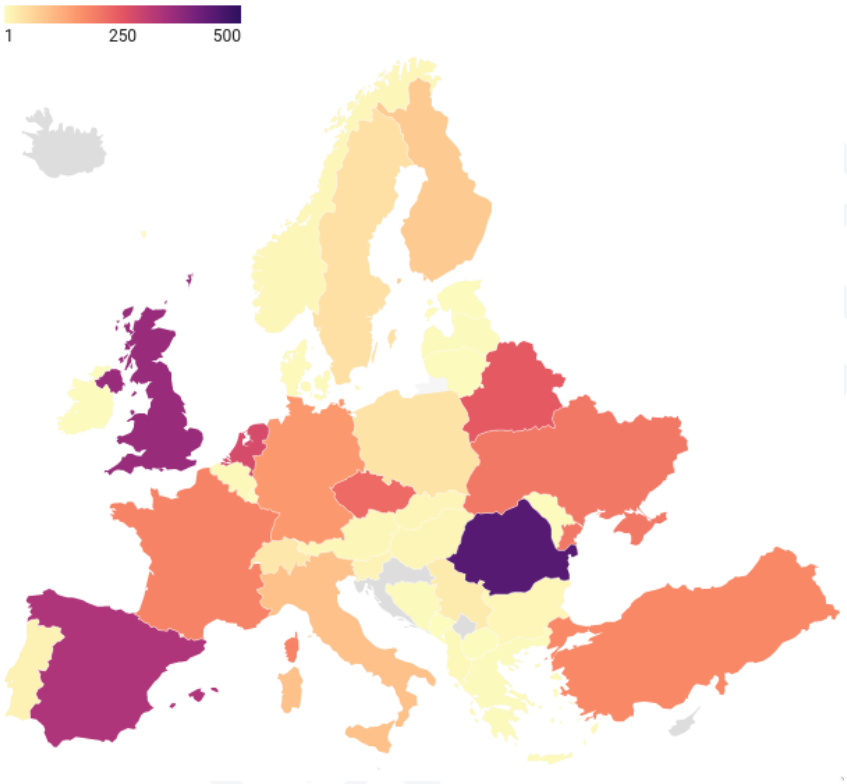


Figure 10. Victim distribution in Europe.

It is worth noting that the majority of IP addresses, TA505 uses to manage and operate **ServHelper** software belong to a hosting company located in Moldova (MivoCloud SRL), while most of its EU-based victims are located in Romania. The two countries share a common language and culture, yet are are on very different geopolitical terms. Investigators have linked TA505 activities to Eastern Europe in the past, but this is an important new piece of evidence linking the group to a specific country.

TA505 has already demonstrated its preference for opportunistic financial gain over political motivations. It's possible that Romanian victims simply make easy targets for Moldavian threat actors due to their shared language and culture, but this conjecture is based on circumstantial evidence.

5 Conclusion

ServHelper is an example of backdoor malware runs by a financially motivated and highly sophisticated threat group. TA505 appears to be well-embedded in the international cybercrime community, as demonstrated by its ability to collect and sell RDP connections to victim devices. The PTI team was able to gain valuable insight into how TA505 organizes its activities and achieves its goals. This will help cybersecurity policies to protect against backdoor attacks like **ServHelper**.

From how TA505 commented their victims on TeslaGun panels perspective, it is obviously seen that TA505 is actively searching for online banking and shopping accounts, particularly from victims in the United States, but also from Russia, Romania, Brazil, and the UK. The threat group will also attack victims outside of its primary scope, tagging RDP connections for eventual resale to other cybercriminals. Ultimately, anyone could be a TA505 victim.

The PTI team observed that TA505's internal structure is surprisingly disorganized. TeslaGun panels are not exclusively separated by campaign and do not include individual victim detail pages. Despite this fact, TA505 members carefully monitor their victims and can demonstrate remarkable patience, especially with high-value victims in the finance sector.

In spite of loose internal organization, TA505 is highly proactive when it comes to updating its malware. It can run multiple malware campaigns simultaneously and will frequently update its tools and techniques to evade detection. These campaigns may include unique tools and concepts that are not found in other campaigns[3]. The group's agility can make it difficult to predict and hard to detect over time.

The group does exhibit some telltale weaknesses, however. While TA505 can maintain hidden connections on victims' devices for months, its members are often unusually noisy. After installing **ServHelper**, TA505 threat actors may manually connect to victim devices through RDP tunneling. Security technologies capable of detecting these tunnels may prove vital for catching and mitigating TA505's backdoor attacks.

Proactive detection strategies are critical for overcoming fast-moving threats like TA505 backdoor attack campaigns. Broadly defined prevention-based security may help mitigate some of the most obvious threats, but the reality of today's mature, organized cybercrime industry requires a new strategy. Business leaders and cybersecurity decision-makers must actively search for new cybercrime trends and implement solutions for patching new vulnerabilities in their networks.

6 IOCS

6.1 Domains

```
aasfhhvyyayssa.xyz
aasouv636d.cn
afggaiir3a.xyz
aisiciciaisxuusuxic.xyz
aonvjvisi3949vnao30cv.xyz
aosdnvnauurt.xyz
asdijoisad87ay3.cn
asdyyauscuauusc.xyz
asfggagsa3.xyz
asfjjasguasus.xyz
asfjjsdvv33gqrr2fv.cn
asfpihbhbyd.xyz
asfuuvhv3083f.xyz
asgyyya6ychcha.xyz
asudjasdusad.xyz
dfsrakizimoy34ggf.xyz
dkaknvizisic.xyz
hitnaiguat.xyz
listjhueaa.cn
neboley.cn
novacation.cn
pgf5ga4g4b.cn
pssoduvnzud.xyz
sacmmvivuasd.xyz
sadiviai9d9asd.xyz
sagbbrrww2.cn
sagiai3agar.cn
saidifufaysydas.cn
saidijfjv9as.xyz
saidiviaiisj3.xyz
sasdmvica883fen.xyz
sasf6asf683jfsd.xyz
saudjyyvv663.xyz
sdgububue3.xyz
soajfvhv235ua.xyz
whereihjeu3.xyz
teahgiaj3ig.cn
```

6.2 HRDP Tool

755549aead02c8b524e31f9c511ca4395bdcae8c465e3298b90152ec8b8a6ae0
Domain : bromide.xyz

6.3 ServHelper

```
a1219acec7d8b85c7b4626536074eeff8db803b50f60e6f87eaa4289b9e4d326
1b3740d9a8511ddfdb657cd796c7bd0adb49bf8f63490df0248ff07d19cd4294
da012f669961c3631b10dd147f38ca34796c40692e01b51dd206f6a5b755e605
d7ef71aa67e1fb5a364c97ff4b89f5f6a28db1c84f91563547a4e44581833486
4ff1dae2285660a46c356a8e836879adc2999f2044a26d17ac4ce5f9e1b442a3
f771432c3652882bb0a7ddf235648c606f713f6f5baf610358784ffb84be8119
13520de2d217cc8b84b80c9ddf7d63173cb086ef731aecf305aef8cc1822bf7d
f62434d2bfd1b9d953618d0be4ba442e3210b821575ae1b1c97ae6aa55ae394a
86e2c0d8edca2f757546e0a39ad127a765baadd1bdfd4684989c2f48e91191af
345c8cfc9b89b30c742e78d7d57b706a2964d5be97fa95b69f2f3eb58d32db63
7d2e5d0e384590ef4f759d93c19400f2914247774ae95c79f24051f3d2a3008e
1445bf709e6a8d940bad6be531c783b2429132b61998d5797ea818847efa1d7b
5c9d696efa6dc5c89e8aa672cbd94d871876ef7aeb0f59a641ac13db7764363e
8c3488033b807907447020614326208845 47c91ea3c4862acb220625eba77024
b075e0ab2910952131b06aee792fed4c97bcdc7f5817112f3035308cd4636c4c
02dcc8523e47914f0ff7f9eb632c0f317960271b4f5161b27e09937deef83b07
87c765c5fce805243bb8c87424235b4fc08fdf0f47517a302dc40583632904d0
97c3090d1be0ac549a065eb7346cbe5052d7c10040f6d44e3cd082f84ded618e
9bb4fdc2f141a11fa7ea8a6e1a6754593d1e85ae29d64d46d72fc8da1dae3bb1
25b987d4f4017e0e97c4b81eeab59c4fcf7832dc48a8e7f12ae5184ccc229937
151f8b796850f46dc292cd7153a68cc7efe4dd694e2164087b42023b4dacc8c3
ceeebe176e8e2d2eccbcb66aa2dd78acbd461d912123114d33526089ae7f2e6f
d541b9ff1fd68818abd9d0f70966e97beaab82dd6bb32d66566fbd6d657fbfd8
6f76d29b00e83d8fef479e9e261e4fe8f98db387c15d8d8bfebbe03b898c0131
64cb280711db0137dc6da7f2cd71745f94ada56d890c6326f07f1b36eee36e07
b32f96217e69b983264075a884c789bbb59b04995f5468c2c6a54d9385d13a80
b2c81b6b95ad45e343ad9376c11c9243f810bd99bb3b8d140eaa4ae2f2444f8c
e04abdb57ce06940bdbac3b5c6a99a7e52e6c315dd97e3da045d570871e7900b
d62856d3faa446b2b0305691aa0a1cb4d03c12e24a6581285a25b15e10b5cc67
3c441477158518c9994e3b42f49278cb0e4f048fcc2648f21f0816cf77187445
a09dcec94458d1970ded54ec374167cd227fea6ff4b56effa1755926d7bd5f41
6f76d29b00e83d8fef479e9e261e4fe8f98db387c15d8d8bfebbe03b898c0131
282e8186cec5ec821d89c7347f508aca3eb1e5c532200d50550e75972e5c33c8
59562b8cc45655a72f7b54e1de28c5585d1d6ccf2963b73d8737ecc2387aeb1b
f0a360fac55b952594568dadd94d7a60d575893fa9258314f098a9e98df45bae
cc28e327610e9deb6551c99a32a44fec86220f2840276474ded747580af850d3
3db7b97aa0bff0fdde441f01d62d0504c33088314472a3cbbd6bc684dd04697b
1557c247f197086be4a5076f89b88357a9a5ecb7dbb3de2d0cf63eda57a24d7a
6839de9e0b5882b0e6668bc5e68b23923be40efaf2bd3606caf71f66aaf01478
f3b0f09bea01f4577516594f646ab3c05f5829aafad7e42370ed97ac95b5df58
6377077d1743520bec5e8c287d56e6f443cb40201450252a880d5fee7271b151
f3b0f09bea01f4577516594f646ab3c05f5829aafad7e42370ed97ac95b5df58
b5e776f84f8f01fcc1fb822ff5612afe62097bf367ced2187fda0b5bf3d652ee
5911ad0a2f2f76cbe6e83b58b95ac820aee88b7fb37e017275bd3984b3b92bfa
```

```
fc3c17833725d727590ef00fdf3f8d70f52d4c13a9cf52a77b6e74e22d7dae61
046f08e500cc9156c4af47a73744ccb060606c77d7a8beb5677aa6ff4d256211
0d8119421ceeffeab9c6bbb649eb52e8d6f0fb049fa0293166af3d65cfa1489e
7fae4ffb43200001f2f16a6a2b23a507370fb692c8fa659d3c335fb7a4002277
c7cb1cc9a2148e8db293de61d791cbbe7202eda89335c93caf454028a61d0a90
353a484824356a70e6d08c5cf637228d2788364199c1bb4b3feca28783378f74
2fd386c26b8a516a4cd864d59df2c74321f3e0436ca4e876a42c4e34f56ae074
08a75beea96e15a6bc2e838cf0649ef0e3be100b819d4513b816778f18903c12
60fc94385520b4353ddc0d9fda9698f4f61ff74abaf794525b9828f8bc24ed0a
c2e0d82381c56792d5dc7d3288bbeb68b53c8d6bfad4c22f33bab9ad5bb848e0
8190afb8cbe829cdf4aca9351e5a772e228a4afcd9f04c55f2e3cd23a2d185ab
a14ccd32d63e5ae6638980c12aaec19aeb86646ac5fc3d0f8fc9042ce11e48af
d8ebd1d13056d7ae44d84ddcf7df37b79940a89918aa7871f36241de65c624ad
3ebf679771812224bfa18e2736116a8e5d811191e0ef5c9639fa853032d52cc0
a2b0ef2413399dbdb01de3a0d2dd310ba127bbfdad09352fecb8444d88a05662
ed29d4ab1988cb5066a313d0d0b08459899ecbd827df42d4e171bad0f3717448
26235babec09882e22c83a2862221c670dd1ca690a76cf1c313842a0c8ae4af3
216f34056b57137d69073604206e30a606188c6c42bdd24d08643266cd631e2a
6a68a6a3ccb8db1621e0655385c566969ff356b5fa6da357d9d098788a32cfa5
9ec2cdb88e31593abc176a5b11c7993d3039444f9dcfd607c1bf1bcc9db939b3
4ff9ad975fec22dd387c910dc163a2cfe3fffe7152b6f97d597ccb936caaab99
11327ae9126f1e924e43dbb06a5e3d158d4d980472f0f2f30f9f73443913776d
7af3f4589a0d13da9f6f09244cd02fca406632e55a02648371978b047bf3647b
5cabe27ecb16899c66c118077e9574191d29671c8136a8274addf6fa1cd103c7
64f1a2f9b95a39c04b60062a24a7bc6de038f706cd679df7b1346c34c055e0b1
0bc24531345dd120b7242992dd2a00429c62535adfd8f69041431ac9ae13793d
c0516809e105193c11ac5913c57c3aacfbfaa98e046bdd8ab9f71c1d555f0534
6e43a01b09534fe3932ebc9d0ea950baeb28bf00cd157b618c8ec4ba6f346c66
9530ff957cd2b657cf8ee3b315636b6ef6124ecc785e9b769618043ed5c561bb
7a58242ae37aab93f74185733ffd30425ca9d2451c83655aa2c07c09b5f40f90
7ed9b5536d19ad840881d068719dbc95da230bf00ba647bf1340bc5666daf2c7
00a8e4ff48e955d37146ea6994812b3bdfecdff356d5fcdd1b23e5aedfb39604
7f6e55013ecda2d56a70b135b412943aec62ba6bf314356b7c518215ce1d7d15
00a8e4ff48e955d37146ea6994812b3bdfecdff356d5fcdd1b23e5aedfb39604
5fd42aaad58f4a1377fd528dbe6010b014b2e922243942ed00df9a8ed7ed33b9
9c1643a07c97b89e8b9fbdf0ea661f98549cfaca9478d1b87ae52eee79e06567
f78d5aecc88c20ad1121ce0b504eb8de51e461e1b3820db07577906649841bdc
```

6.4 RDP/Proxy Servers

```
37.1.201.136
5.61.60.54
23.227.194.159
```

6.5 Management Panels

```
185.163.45.186
185.163.45.240
185.163.45.248
185.163.45.56
185.163.47.171
185.163.47.210
194.180.174.20
194.180.174.56
206.188.197.203
206.188.197.221
5.181.156.142
5.181.156.15
5.181.156.4
5.181.156.64
94.158.245.113
94.158.245.172
94.158.245.180
94.158.245.73
94.158.245.77
```

7 TTP List - MITRE ATT&CK Codes

1. Execution
   (a) T1047 - Windows Management Instrumentation
   (b) T1053 - Scheduled Task/Job
   (c) T1053.005 - Scheduled Task
   (d) T1059 - Command and Scripting Interpreter
   (e) T1059.003 - Windows Command Shell
   (f) T1059.001 - PowerShell
2. Discovery
   (a) T1033 - System Owner/User Discovery
   (b) T1069 - Permission Groups Discovery
   (c) T1069.001 - Local Groups
   (d) T1082 - System Information Discovery
3. Persistence
   (a) T1547 - Boot or Logon Autostart Execution
   (b) T1547.001 - Registry Run Keys / Startup Folder
   (c) T1053 - Scheduled Task/Job
   (d) T1053.005 - Scheduled Task
   (e) T1136 - Create Account
   (f) T1136.001 - Local Account
4. Privilege Escalation
   (a) T1547 - Boot or Logon Autostart Execution
   (b) T1547.001 - Registry Run Keys / Startup Folder
   (c) T1053 - Scheduled Task/Job
   (d) T1053.005 - Scheduled Task
5. Command And Control
   (a) T1071 - Application Layer Protocol
   (b) T1071.001 - Web Protocols
   (c) T1572 - Protocol Tunneling
   (d) T1090 - Proxy
   (e) T1090.002 - External Proxy
   (f) T1573 - Encrypted Channel
   (g) T1573.002 - Asymmetric Cryptography
   (h) T1105 - Ingress Tool Transfer
6. Defense Evasion
   (a) T1036 - Masquerading
   (b) T1036.004 - Masquerade Task or Service
   (c) T1036.005 - Match Legitimate Name or Location
   (d) T1036.001 - Invalid Code Signature
   (e) T1218 - Signed Binary Proxy Execution
   (f) T1218.011 - Rundll32
   (g) T1070 - Indicator Removal on Host
   (h) T1070.004 - File Deletion
7. Lateral Movement
   (a) T1021 - Remote Services
   (b) T1021.001 - Remote Desktop Protocol

Références

[1] Binary Defence. *An Updated ServHelper Tunnel Variant*. url : https://www.binarydefense.com/an-updated-servhelper-tunnel-variant/. (accessed : 26.11.2021).

[2] Binary Defence. *TA505 is back with new ttps and updated flawedgrace RAT*. url : https://www.binarydefense.com/threat_watch/ta505-is-back-with-new-ttps-and-updated-flawedgrace-rat. (accessed : 26.11.2021).

[3] NCC Group. *Tracking a P2P network related to TA505*. url : https://research.nccgroup.com/2021/12/01/tracking-a-p2p-network-related-with-ta505/. (accessed : 5.01.2022).

[4] Cisco Talos Intelligence. *Signed MSI files, Raccoon and Amadey are used for installing ServHelper RAT*. url : https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html. (accessed : 26.11.2021).

[5] MITRE. *TA505*. url : https://attack.mitre.org/groups/G0092/. (accessed : 26.11.2021).

[6] ProofPoint. *ServHelper and FlawedGrace - New malware introduced by TA505*. url : https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505t. (accessed : 26.11.2021).

Acknowledgement
We would like to thank our advisors for their valuable guidance and support throughout this research.

The readers can find new samples, IOCs, and new versions of this report from our https://github.com/prodaft/malware-ioc page as we will constantly update it based on new findings.

Historique

Version	Date	Auteur(s)	Modifications
1.0	19.01.2021	PTI Team	Initial TLP:RED draft
1.1	02.05.2021	PTI Team	Initial TLP:RED LE version
1.2	26.11.2021	PTI Team	Enrichment
2.0	22.04.2022	PTI Team	Updated TLP:RED LE version
3.0	05.09.2022	PTI Team	Redacted TLP:WHITE version