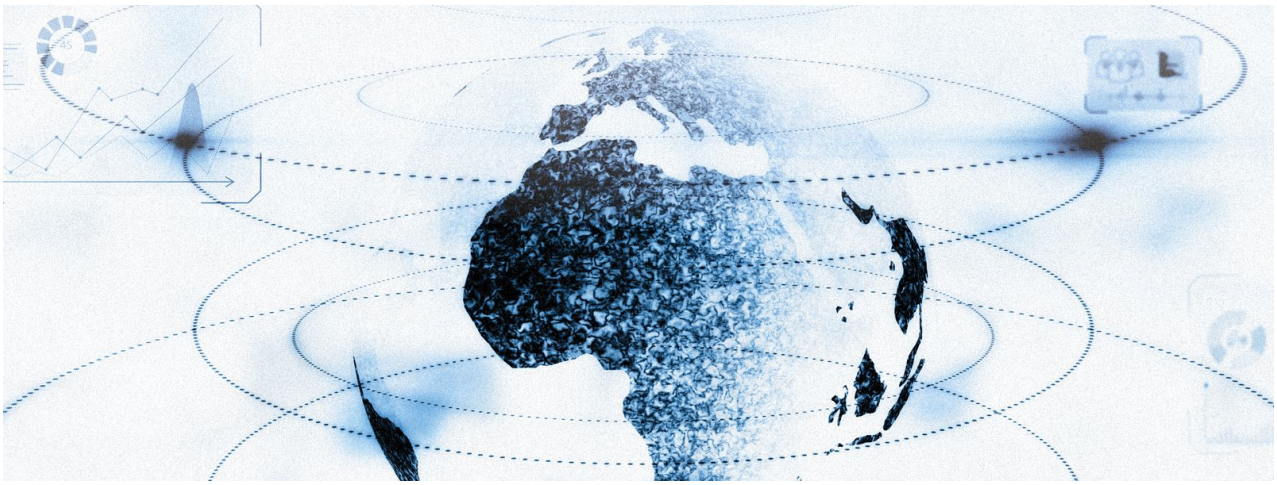
Exposing TAG-53's Credential Harvesting Infrastructure Used for Russia-Aligned Espionage Operations

recordedfuture.com/exposing-tag-53-credential-harvesting-infrastructure-for-russia-aligned-espionage-operations

Research (Insikt)

Posted: 5th December 2022

By: Insikt Group®



Editor's Note: Click here to download the report as a PDF.

This report profiles the infrastructure used by the threat activity group TAG-53, which overlaps with public reporting on Callisto Group, COLDRIVER, and SEABORGIUM. The activity was identified through a combination of Network Intelligence and analysis derived from open-source reporting. The report will be of most interest to network defenders and individuals engaged in strategic and operational intelligence relating to the activities of the Russian state in cyberspace.

Executive Summary

Beginning in July 2022, Recorded Future's Insikt Group observed the recurring use of similar infrastructure by the threat activity group TAG-53. This newly discovered infrastructure likely overlaps with other infrastructure tactics, techniques, and procedures (TTPs) previously attributed to Callisto Group, COLDRIVER, and SEABORGIUM, who have been linked to activity aligning with Russian state interests.

Insikt Group has observed the recurring use of common traits by TAG-53 when curating its infrastructure, including the use of domain names employing a specific pattern construct along with Let's Encrypt TLS certificates, the use of a specific cluster of hosting providers, and the use of a small cluster of autonomous systems.

TAG-53 infrastructure was found to contain a spoofed Microsoft login page masquerading as a legitimate military weapons and hardware supplier in the United States, suggesting that some TAG-53 infrastructure has likely already been operationalized. Based on historical public reporting on overlapping TAG-53 campaigns, it is likely that this credential harvesting activity is enabled in part through phishing.

Key Judgments

- Insikt Group has identified new infrastructure used by TAG-53, a group likely linked to suspected Russian threat activity groups Callisto Group, COLDRIVER, and SEABORGIUM.
- The identified TAG-53 infrastructure features common traits including the use of specific domain registrars, the use of Let's Encrypt TLS certificates, and a small cluster of autonomous systems. Most of TAG-53's domains use a specific stylistic structure.
- TAG-53 has used domains masquerading as organizations across multiple industry verticals, with a particular focus on government, intelligence, and military industries.

Background

TAG-53 is consistent when setting up its infrastructure, which bears significant hallmarks and crossover with infrastructure attributed to Callisto Group, COLDRIVER, and SEABORGIUM. The group continues to use particular stylistic structures when registering malicious domains alongside the use of specific domain registrars with IP addresses that reside in a small cluster of autonomous systems.

On August 15, 2022, a Microsoft report published in collaboration with Google's Threat Analysis Group (TAG) and Proofpoint's Threat Research Team detailed SEABORGIUM's phishing operations. In this research, Microsoft assesses that SEABORGIUM originates from Russia and has "objectives and victimology that align closely with Russian state interests". Microsoft denotes that SEABORGIUM shares overlaps with Callisto Group, TA446, and COLDRIVER and indicates that the threat actor has carried out persistent phishing and credential theft campaigns that have led to intrusions and data theft. SEABORGIUM primarily focuses its targeting on NATO countries, including a specific emphasis on the United States and the United Kingdom. The group also targeted Ukraine in the run-up to Russia's full-scale invasion of the country in February 2022.

Google's TAG reported in March and updated in May 2022 that COLDRIVER has conducted credential phishing campaigns using Gmail accounts targeting nongovernmental organizations and think tanks, journalists, and government and

defense officials. TAG also suggests that COLDRIVER's TTPs have evolved over time, moving towards incorporating PDF or DOC file links that are hosted on Google Drive and Microsoft OneDrive within its phishing emails.

Threat and Technical Analysis

Insikt Group used intelligence provided in open-source reporting (1, 2, 3, 4) to profile TAG-53 infrastructure that likely overlaps with Callisto Group, COLDRIVER, and SEABORGIUM infrastructure. TAG-53 infrastructure was uncovered by analyzing specific combinations of domain registrars, autonomous systems, domain name structures, and related TLS certificates. Based on this information, it is highly likely that this threat group is continuing its phishing and credential-harvesting operations. While monitoring TAG-53 infrastructure, Insikt Group observed a spoofed Microsoft login page masquerading as a legitimate military weapons and hardware supplier in the US, suggesting that some TAG-53 infrastructure has likely already been operationalized.

Registrars

Using both current and passive Domain Name System (DNS) records, Insikt Group resolved IP addresses for 38 registered domains used by TAG-53 since January 2022. The identified TAG-53 domains, listed in Appendix A, have highlighted a trend towards the use of NameCheap, Porkbun, REG.RU, and regway for domain registration that has persisted since mid-2022, a breakdown of which can be seen in Figure 1. The reason for the preference of these registrars is unknown, but it is a useful metric when profiling candidate TAG-53 infrastructure.

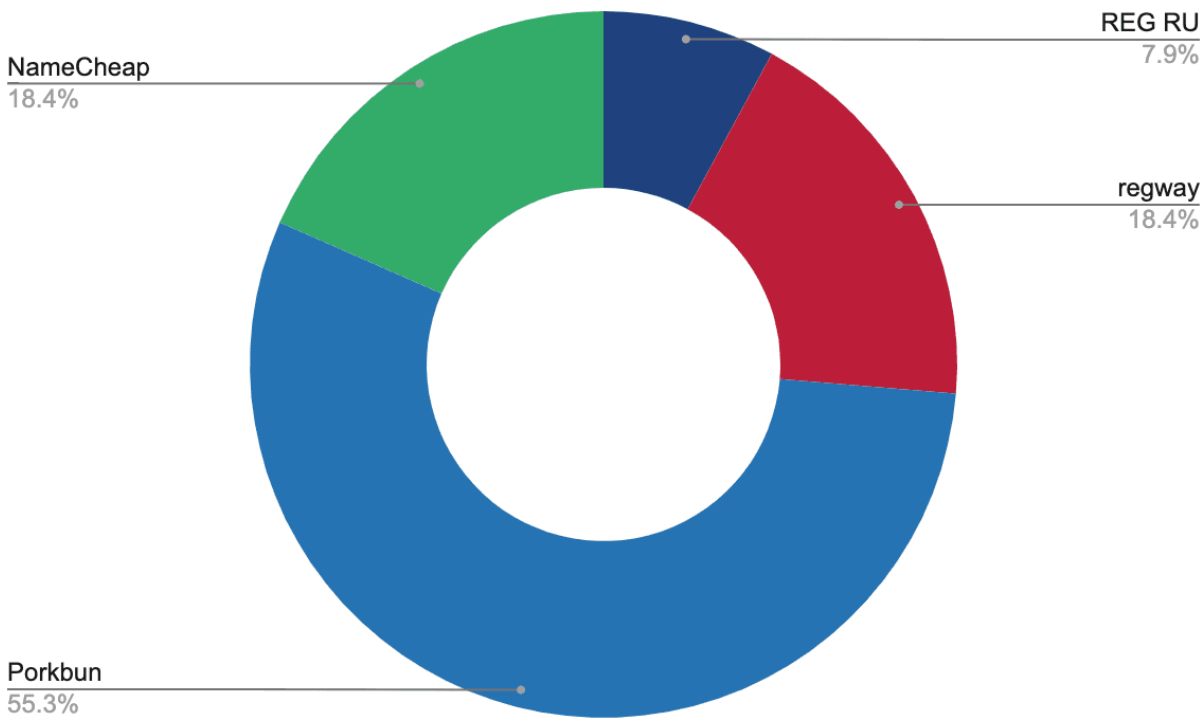


Figure 1: Breakdown of domain registrars used by TAG-53 since January 2022 (Source: Recorded Future)

Autonomous Systems

Alongside the use of specific domain registrars is the use of particular autonomous systems, with all domains collected under TAG-53 found to exist in 10 autonomous systems with a significant concentration found located in 2 Autonomous System Numbers (ASNs) linked to MIRhosting (AS52000) and Hostwinds (AS54290) shown in Table 1 below.

ASN	AS Name	TAG-53 Domain Count
AS52000	MIRhosting	11
AS54290	HOSTWINDS	10
AS44094	WEBHOST1-AS	4
AS62240	Clouvider	4
AS62005	BV-EU-AS	3
AS44477	STARK-INDUSTRIES	2
AS16276	OVH	1
AS20278	NEXEON	1
AS206446	CLOUDLEASE	1
AS43624	STARK-INDUSTRIES-SOLUTIONS-AS	1

Table 1: ASN detail breakdown for TAG-53 linked domains (Source: Recorded Future)

Domain Name Structure

Most of the domains discovered via TAG-53 tracking use similarly structured domain names, primarily made up of 2 terms separated by a hyphen, such as “cloud-safety[.]online”. Of the 38 domains identified, 33 used the stylistic form “-.(com|online|ru)”. Of the remaining 5 domains, 4 were found to be similar, but consisted of 3 terms and 2 hyphens — “share-drive-ua[.]com”, “network-storage-ltd[.]com”, “land-of-service[.]com”, and “nonviolent-conflict-service[.]com” — and 1 contained no hyphens — “proxycrioisolation[.]com”. However, additional factors enabled Insikt Group to link these domains to the rest of TAG-53’s infrastructure.

A breakdown of the terms found in TAG-53 domains, shown in Figure 2, highlights the repeated use of specific words within the domains, most of which are common, generic computing terms.

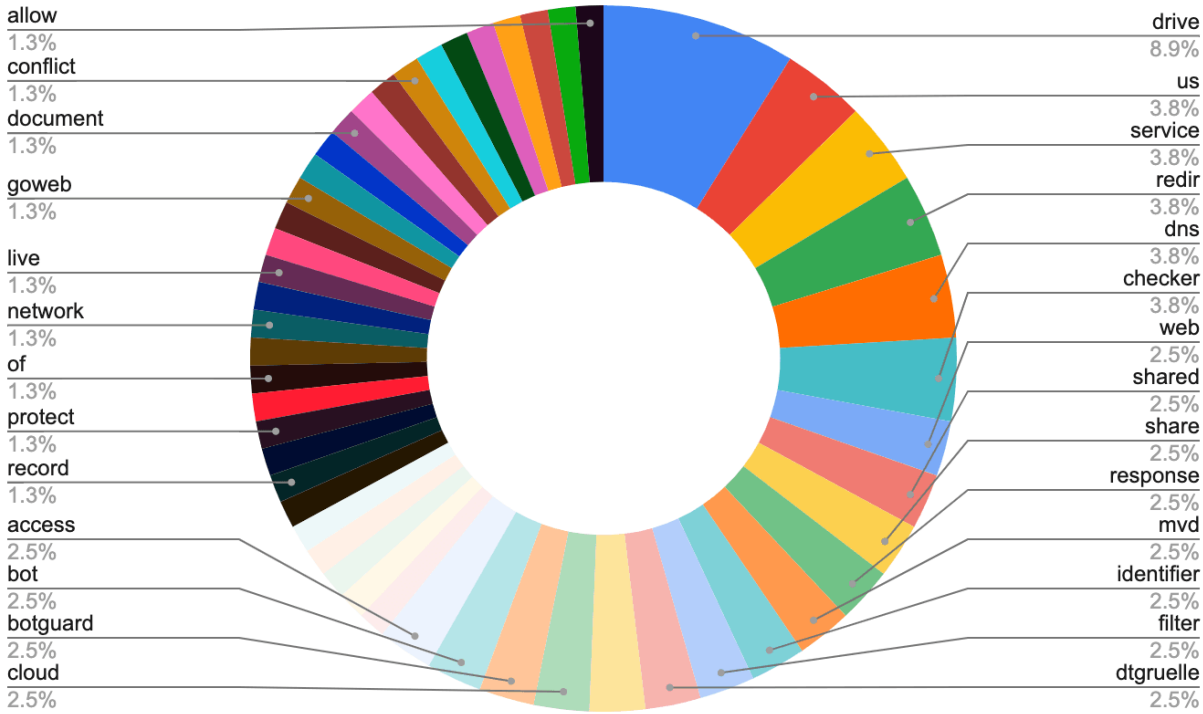


Figure 2: Breakdown of terms used in TAG-53 linked domains (Source: Recorded Future)

X.509 TLS Certificates

All identified TAG-53 domains were found to host corresponding X.509 TLS certificates provided by Let's Encrypt, an example of which is shown in Figure 3. The prevalent use of Let's Encrypt TLS certificates allows for further correlations between TAG-53 domains and infrastructure, strengthening the clustering of this activity.

```
Data:
    Version: 3 (0x2)
    Serial Number:
        03:05:f7:75:16:d1:98:1d:a0:bc:47:e8:89:20:94:fe:40:4a
    Signature Algorithm: ecdsa-with-SHA384
    Issuer: (CA ID: 183283)
        commonName               = E1
        organizationName         = Let's Encrypt
        countryName              = US
    Validity
        Not Before: Oct  3 16:47:32 2022 GMT
        Not After : Jan  1 16:47:31 2023 GMT
    Subject:
        commonName               = *.drive-globalordnance[.]com
    Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
    ...
```

Figure 3: Partial X.509 TLS certificate for drive-globalordnance[.]com (Source: crt.sh)

Targeting and Victimology

Of the 38 discovered domains, 9 contained references to potential target organizations or organizations that TAG-53 may be attempting to masquerade as, shown in Table 2. The reason behind the use of these themed domains is not fully understood beyond the likely attempt to emulate real entities in order to appear more legitimate to potential targets and victims.

TAG-53 Domain	Suspected Target/Masquerade	Industry Vertical
umopl-drive[.]com	UMO Poland	Aerospace and Defense: Hardware/Weaponry
drive-globalordnance[.]com	Global Ordnance	Aerospace and Defense: Hardware/Weaponry
sangrail-share[.]com	Sangrail LTD	Aerospace and Defense: Military & Civilian Intelligence
dtgruelle-us[.]com	DTGruelle	Logistics
dtgruelle-drive[.]com		
cija-docs[.]com	The Commission for International Justice and Accountability (CIJA)	NGO: Armed Conflict Crime Investigations
blueskynetwork-shared[.]com	Blue Sky Network	Telecommunications: Satelite
dns-mvd[.]ru	The Ministry of Internal Affairs of the Russian Federation (MVD)	Government: Russian Ministry of Internal Affairs
mvd-redir[.]ru		

Table 2: Suspected targets/masquerades of TAG-53 linked domains (Source: Recorded Future)

Analysis of the 9 domains reveals that 7 share a focus around industry verticals that would likely be of interest to Russia-nexus threat groups, especially in light of the war in Ukraine. The 2 outlier domains are probably intended to masquerade as the Ministry of Internal Affairs of the Russian Federation. (MVD)

Credential Harvesting

The TAG-53 domain “drive-globalordnance[.]com” includes a spoofed sign-in page for the legitimate company Global Ordnance, a military weapons and hardware supplier in the US. The spoofed sign-in page, shown in Figure 4, uses Global Ordnance branding and is suspected to be used for follow-on credential harvesting after a target has been phished. It

is unclear whether Global Ordnance is the intended target of this attempted credential harvesting operation or whether TAG-53 is using a Global Ordnance-styled domain and spoofed sign-in page to masquerade as a legitimate entity to target victims.

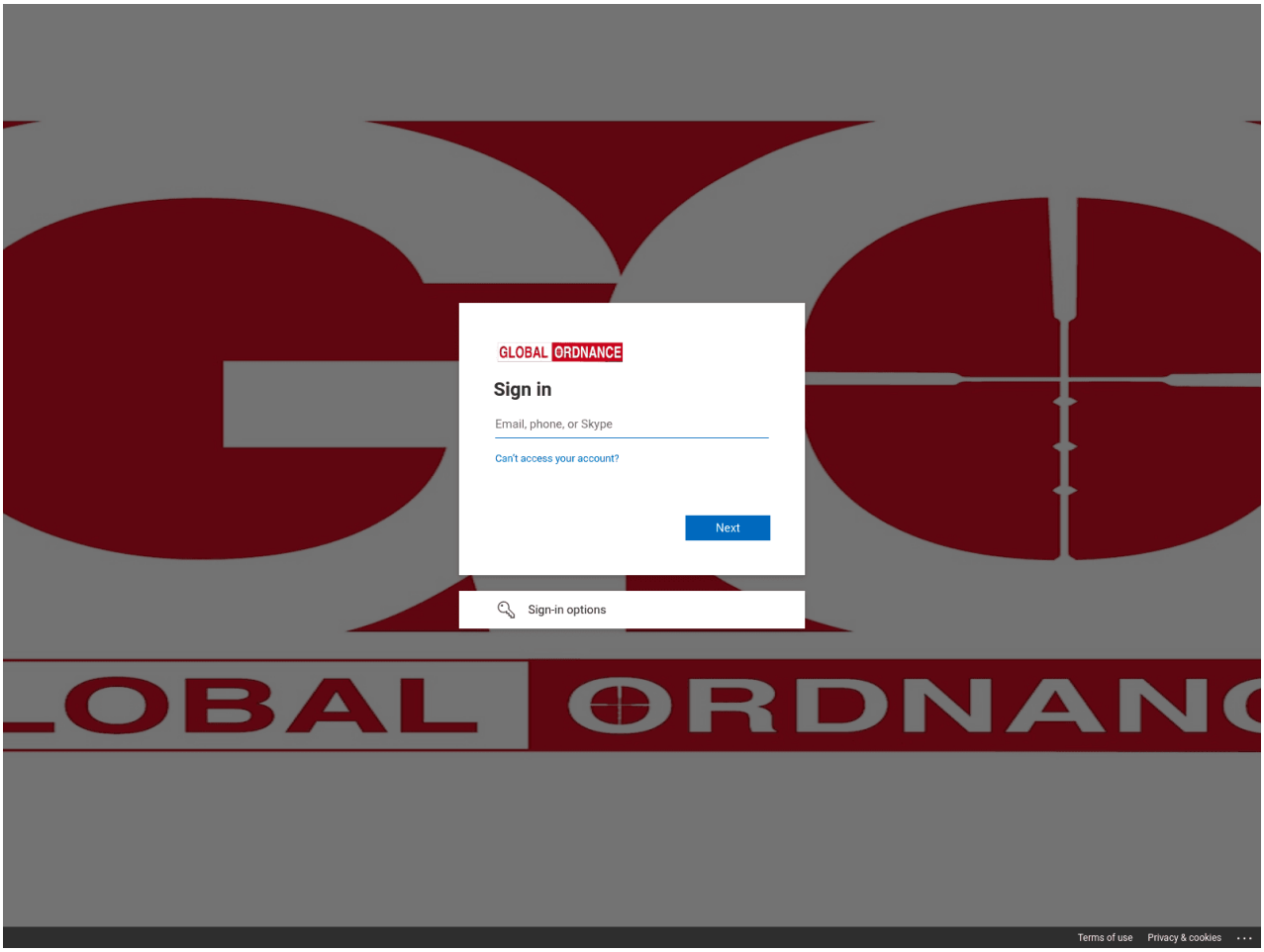


Figure 4: TAG-53 Global Ordnance spoofed sign-in page (Source: URLScan)

Mitigations

Users should conduct the following measures to detect and mitigate activity associated with TAG-53:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Recorded Future proactively detects malicious server configurations and provides means to block them in the Command and Control Security Control Feed. The Command and Control Feed includes tools used by TAG-53 and other Russian state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.

- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence modules users can monitor real-time output from Network Intelligence analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence (BI) module. The SecurityTrails extension is available to any customer that has a subscription to the Threat Intelligence or Brand Intelligence modules. The LogoType source and alerting is exclusive to the BI module, though the TI module does have access to the data via the Advanced Query Builder.
- Recorded Future's Fraudulent Domains and Typosquats playbook explains triaging typosquatting or similar domain alerts. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.

Outlook

Insikt Group continues to track TAG-53 infrastructure and observe changes in TTPs as the group's credential harvesting operations diversify. Notably, a consistent trend has emerged regarding the use of specifically tailored infrastructure by TAG-53 highlighting the long-term use of similar techniques for their strategic campaigns.

Readers should detect, block, and hunt for the indicators referenced in connection with TAG-53 reporting via the Recorded Future Platform in network monitoring, intrusion detection systems, firewalls, and any associated perimeter security appliances.

Appendix A — Indicators

Domains

access-confirmation[.]com
allow-access[.]com
antibots-service[.]com
blueskynetwork-shared[.]com
botguard-checker[.]com
botguard-web[.]com
challenge-identifier[.]com
checker-bot[.]com
cija-docs[.]com
cloud-safety[.]online
cloud-us[.]online
dns-cache[.]online
dns-cookie[.]com
dns-mvd[.]ru
docs-web[.]online
drive-control[.]com
drive-globalordnance[.]com

drive-previewer[.]com
drive-us[.]online
dtgruelle-drive[.]com
dtgruelle-us[.]com
encompass-shared[.]com
filter-bot[.]com
goweb-protect[.]com
guard-checker[.]com
land-of-service[.]com
live-identifier[.]com
mvd-redir[.]ru
network-storage-ltd[.]com
nonviolent-conflict-service[.]com
proxycrioisolation[.]com
redir-document[.]com
response-filter[.]com
response-redir[.]com
sangrail-share[.]com
share-drive-ua[.]com
transfer-record[.]com
umopl-drive[.]com

IP Addresses

23[.]254[.]201[.]243
45[.]66[.]248[.]9
45[.]86[.]230[.]198
45[.]153[.]229[.]79
64[.]44[.]101[.]31
77[.]91[.]126[.]16
77[.]91[.]126[.]35
77[.]91[.]126[.]46
77[.]91[.]126[.]62
77[.]91[.]126[.]64
77[.]91[.]126[.]66
77[.]91[.]126[.]69
77[.]91[.]69[.]109
85[.]239[.]53[.]210
85[.]239[.]60[.]18
85[.]239[.]61[.]49
85[.]239[.]61[.]86
138[.]124[.]187[.]143
138[.]124[.]187[.]222
142[.]11[.]209[.]171
142[.]11[.]209[.]180

142[.]11[.]210[.]53
146[.]19[.]230[.]182
146[.]59[.]102[.]76
185[.]164[.]172[.]128
185[.]164[.]172[.]220
185[.]179[.]188[.]73
185[.]179[.]189[.]32
185[.]179[.]189[.]43
185[.]179[.]189[.]45
192[.]119[.]65[.]114
192[.]119[.]97[.]190
192[.]119[.]112[.]249
192[.]129[.]154[.]225
192[.]236[.]195[.]114
192[.]236[.]193[.]194
193[.]200[.]17[.]102
195[.]246[.]110[.]45

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Defense Evasion: Masquerading	T1036
Reconnaissance: Phishing for Information	T1598
Resource Development: Stage Capabilities	T1608