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

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](https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations) 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](https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe) in March and [updated](https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe) 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](https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations), [2](https://blog.sekoia.io/calisto-continues-its-credential-harvesting-campaign), [3](https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe), [4](https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe)) 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.

##### 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)

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 “

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.

##### 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.

##### 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.

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.

#### 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)](https://www.recordedfuture.com/platform/threat-intelligence), [Third-Party Intelligence](https://www.recordedfuture.com/platform/third-party-intelligence), and [SecOps Intelligence](https://www.recordedfuture.com/platform/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)](https://www.recordedfuture.com/platform/brand-intelligence) 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