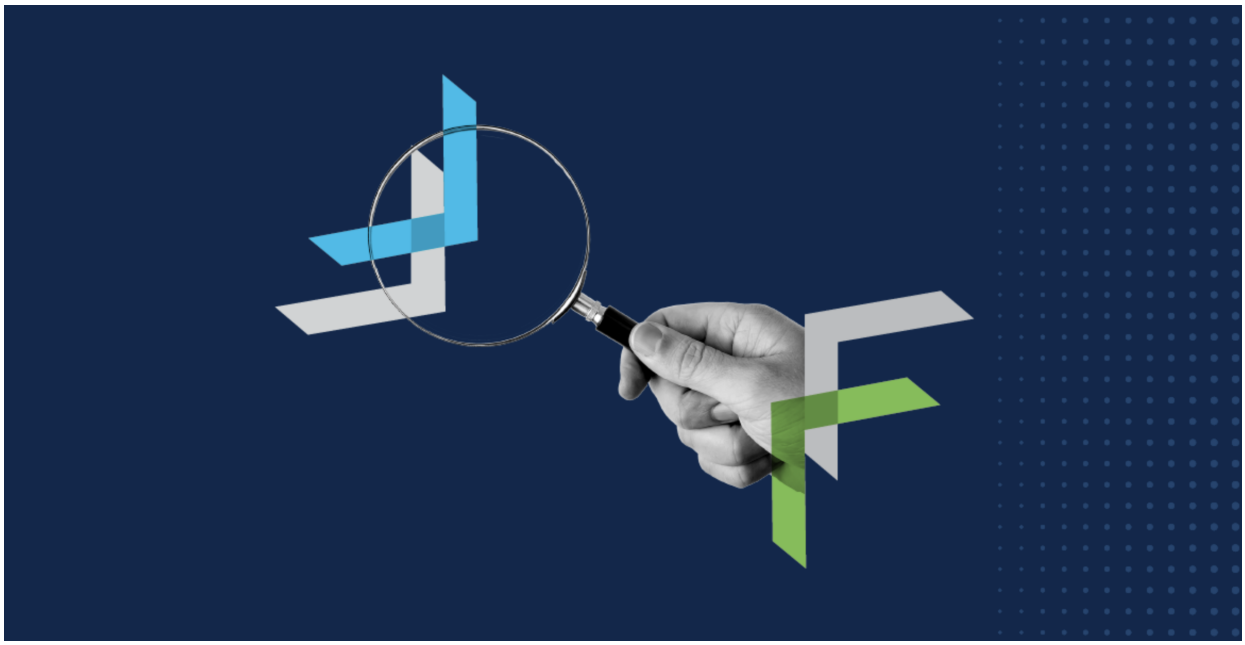
Network Footprints of Gamaredon Group

Onur Mustafa Erdogan ⋮⋮ 5/12/2022



Below research is reflecting our observations during month of March 2022. We also would like to thank Maria Jose Erquiaga for her contribution in introduction and support during the process of writing.

Overview

As the Russian-Ukrainian war continues over conventional warfare, cybersecurity professionals witnessed their domain turning into a real frontier. Threat actors picking sides [1], group members turning against each other [2], some people handing out DDoS tools [3], some people blending in to turn it into profit [4], and many other stories, proving that this new frontier is changing daily, and its direct impact is not limited to geographical boundaries.

While attacks seem to be evolving daily, it is challenging for one to stay up to date with all that is going around. Therefore, we believe that it is important to distinguish between information and actionable intelligence. In Cisco Global Threat Alerts, we would like to share our observations related to this conflict during March of 2022 and discover how we can turn them into actionable intelligence together.

Threat Actors in the Russian-Ukrainian Conflict

Since the rapid escalation of the conflict in 2022, security researchers and analysts have been gathering information regarding the adversarial groups, malware, techniques, and types of attacks implemented [1, 5, 6]. Some of the groups and malware related to the conflict are described in Table 1:

Threat Actor	Malware	Location
Gamaredon **[7]**	Pteranodon **[8]**	Crimea
Sandworm **[9]**	CyclopsBlink **[10]**	Russia
WizardSpider **[11]**	Cobalt Strike **[12]**, Emotet **[13]**, Conti **[14]**, Ryuk **[15]**, Trickbot **[16]**	Russia

Table 1: Threat actors and their relations

Gamaredon

Gamaredon group, also known as Primitive Bear, Shuckworm and ACTINIUM, is an advanced persistent threat (APT) based in Russia. Their activities can be traced back as early as 2013, prior to Russia's annexation of the Crimean

Peninsula. They are known to target state institutions of Ukraine and western government entities located in Ukraine. Ukrainian officials attribute them to Russian Federal Security Service, also known as FSB [17].

Gamaredon often leverages malicious office files, distributed through spear phishing as the first stage of their attacks. They are known to use a PowerShell beacon called PowerPunch to download and execute malware for ensuing stages of attacks. Pterodo and QuietSieve are popular malware families that they deploy for stealing information and various actions on objective [18].

We were able to collect network IoC's related to Gamaredon infrastructure. During our initial analysis, most of the indicators were not attributed directly to any specific malware and they were rather listed as part of Gamaredon's infrastructure. Therefore, we wanted to analyze their infrastructure to understand their arsenal and deployment in greater detail.

Network Infrastructure

The first part of this research is focused on WHOIS record analysis. We observed that Gamaredon domains were dominantly registered by REG[.]RU. Creation dates are going back as early as February 2019 and have a changing pattern for the registrant email. Until August 2020, we observed that message-yandex.ru@mail[.]ru was the main registrant email. Later, it shifted to macrobit@inbox[.]ru, mixed with the occasional usage of message-yandex.ru@mail[.]ru and tank-bank15@yandex[.]ru. Domain creation dates in some of the WHOIS records are as recent as March 2022.

Other than WHOIS information, the domains we observed that were related to Gamaredon campaigns had a distinguishing naming convention. While dataset consisted of domain names (without TLDs) varying between 4 to 16 characters, 70% percent of them were between 7 to 10 characters. Combined with a limited group of top-level domains (TLDs) used (see Table 2), this leads us to a naming pattern for further attribution. Additionally, the usage of TLDs on domain creation seems to be rotating.

TLD	Distribution	TLD Usage
online	42.07%	08/2020-02/2021,02/2022
xyz	29.47%	06/2022-08/2022, 02/2022-03/2022
ru	14.22%	08/2020, 05/2021-02/2022
site	8.94%	07/2020-02/2021
space	2.64%	02/2019-06/2020

Table 2: TLD distribution and time in use

In the case of domain resolutions, we aimed to analyze the distribution of autonomous system numbers (ASN) used by resolved IP addresses (see Table 3). Once more, the owner REG[.]RU is leading the list, owning most of the domains. TimeWeb was the second this time, with 28% of the domains we found to be related to Gamaredon activities. Domains having '. online' and '.ru' TLDs are regularly updating their IP resolutions, almost daily.

Owner	ASN	Popular Networks	Distribution
REG.RU, Ltd	AS197695	194.67.71.0/24 194.67.112.0/24 194.58.100.0/24 194.58.112.0/24 194.58.92.0/24 89.108.81.0/24	45.93%
TimeWeb Ltd.	AS9123	185.104.114.0/24 188.225.77.0/24 188.225.82.0/24 94.228.120.0/24 94.228.123.0/24	28.25%
EuroByte LLC	AS210079	95.183.12.42/32	10.56%
AS-CHOOPA	AS20473	139.180.196.149/32	5.08%
LLC Baxet	AS51659	45.135.134.139/32 91.229.91.124/32	2.23%
System Service Ltd.	AS50448	109.95.211.0/24	1.82%

Table 3: Distribution of IP addresses per ASN and owner

Tooling

After understanding the infrastructure, let's proceed with their arsenal. We looked at associated file samples for the domains through Umbrella and Virustotal. A sample of the results can be seen below. Referring to a file type, we can see that the Gamaredon group prefers malicious office documents with macros. Also, they are known to use Pterodo, which is a constantly evolving custom backdoor [8, 18].

Domain	Hash	Type	Mal
acetica[.]online	4c12713ef851e277a66d985f666ac68e73ae21a82d8dcfcedf781c935d640f52	Office Open XML Document	Gro
arvensis[.]xyz	03220baa1eb0ad80808a682543ba1da0ec5d56bf48391a268ba55ff3ba848d2f	Office Open XML Document	Gro
email-smtp[.]online	404ed6164154e8fb7fdd654050305cf02835d169c75213c5333254119fc51a83	Office Open XML Document	Gro
gurmou[.]site	f9a1d7e896498074f7f3321f1599bd12bdf39222746b756406de4e499afbc86b	Office Open XML Document	Gro
mail-check[.]ru	41b7a58d0d663afcdb45ed2706b5b39e1c772efd9314f6c1d1ac015468ea82f4	Office Open XML Document	Gro
office360-expert[.]online	611e4b4e3fd15a1694a77555d858fced1b66ff106323eed58b11af2ae663a608	Office Open XML Document	Gro
achilleas[.]xyz	f021b79168daef8a6359b0b14c0002316e9a98dc79f0bf27e59c48032ef21c3d	Office Open XML Document	Mac ena Wor Troj
anisoptera[.]online	8c6a3df1398677c85a6e11982d99a31013486a9c56452b29fc4e3fc8927030ad	MS Word Document	Mac ena Wor Troj
erythrocephala[.]online	4acfb73e121a49c20423a6d72c75614b438ec53ca6f84173a6a27d52f0466573	Office Open XML Document	Mac ena Wor Troj
hamadryas[.]online	9b6d89ad4e35ffca32c4f44b75c9cc5dd080fd4ce00a117999c9ad8e231d4418	Office Open XML Document	Mac ena Wor Troj
intumescere[.]online	436d2e6da753648cbf7b6b13f0dc855adf51c014e6a778ce1901f2e69bd16360	MS Word Document	Mac ena Wor Troj
limosa[.]online	0b525e66587e564db10bb814495aefb5884d74745297f33503d32b1fec78343f	MS Word Document	Mac ena Wor Troj
mesant[.]online	936b70e0babe7708eda22055db6021aed965083d5bc18aad36bedca993d1442a	MS Word Document	Mac ena Wor Troj
sufflari[.]online	13b780800c94410b3d68060030b5ff62e9a320a71c02963603ae65abbf150d36	MS Word Document	Mac ena Wor Troj
apusa[.]xyz	23d417cd0d3dc0517adb49b10ef11d53e173ae7b427dbb6a7ddf45180056c029	Win32 DLL	Pter

atlanticos[.]site	f5023effc40e6fbb5415bc0bb0aa572a9cf4020dd59b2003a1ad03d356179aa1	VBA	Pter
barbatus[.]online	250bd134a910605b1c4daf212e19b5e1a50eb761a566fffed774b6138e463bbc	VBA	Pter
bitsadmin2[.]space	cfa58e51ad5ce505480bfc3009fc4f16b900de7b5c78fdd2c6d6c420e0096f6b	Win32 EXE	Pter
bitsadmin3[.]space	9c8def2c9d2478be94fba8f77abd3b361d01b9a37cb866a994e76abeb0bf971f	Win32 EXE	Pter
bonitol[.]online	3cbe7d544ef4c8ff8e5c1e101dbdf5316d0cfbe32658d8b9209f922309162bcf	VBA	Pter
buhse[.]xyz	aa566eed1cbb86dab04e170f71213a885832a58737fcab76be63e55f9c60b492	Office Open XML Document	Pter
calendas[.]ru	17b278045a8814170e06d7532e17b831bede8d968ee1a562ca2e9e9b9634c286	Win32 EXE	Pter
coagula[.]online	c3eb8cf3171aa004ea374db410a810e67b3b1e78382d9090ef9426afde276d0f	MS Word Document	Pter
corolain[.]ru	418aacdb3bbe391a1bcb34050081bd456c3f027892f1a944db4c4a74475d0f82	Win32 EXE	Pter
gorigan[.]ru	1c7804155248e2596ec9de97e5cddcddbafbb5c6d066d972bad051f81bbde5c4	Win32 EXE	Pter
gorimana[.]site	90cb5319d7b5bb899b1aa684172942f749755bb998de3a63b2bccb51449d1273	MS Word Document	Pter
krashand[.]ru	11d6a641f8eeb76ae734951383b39592bc1ad3c543486dcef772c14a260a840a	Win32 EXE	Pter
libellus[.]ru	4943ca6ffef366386b5bdc39ea28ad0f60180a54241cf1bee97637e5e552c9a3	Win32 EXE	Pter
melitaeas[.]online	55ad79508f6ccd5015f569ce8c8fcad6f10b1aed930be08ba6c36b2ef1a9fac6	Office Open XML Document	Pter
mullus[.]online	31afda4abdc26d379b848d214c8cbd0b7dc4d62a062723511a98953bebe8cbfc	Win32 EXE	Pter
upload-dt[.]hopto[.]org	4e72fbc5a8c9be5f3ebe56fed9f613cfa5885958c659a2370f0f908703b0fab7	MS Word Document	Pter

Table 4: Domains, files (hash and type), and malware name associated to the Gamaredon group

After reviewing the behaviors of the associated malicious samples, it is easier to build attribution between the malicious domain and the corresponding sample. IP addresses resolved by the domain are later used to establish raw IP command and control (C2) communication with a distinguishing URL pattern. The following example shows how **1c7804155248e2596ec9de97e5cddcddbafbb5c6d066d972bad051f81bbde5c4** resolves **gorigan[.]ru** and uses its IP address to build a C2 URL (http|https<IP>/<random alphanumerical string>). Therefore, DNS and outgoing web traffic is crucial for its detection.

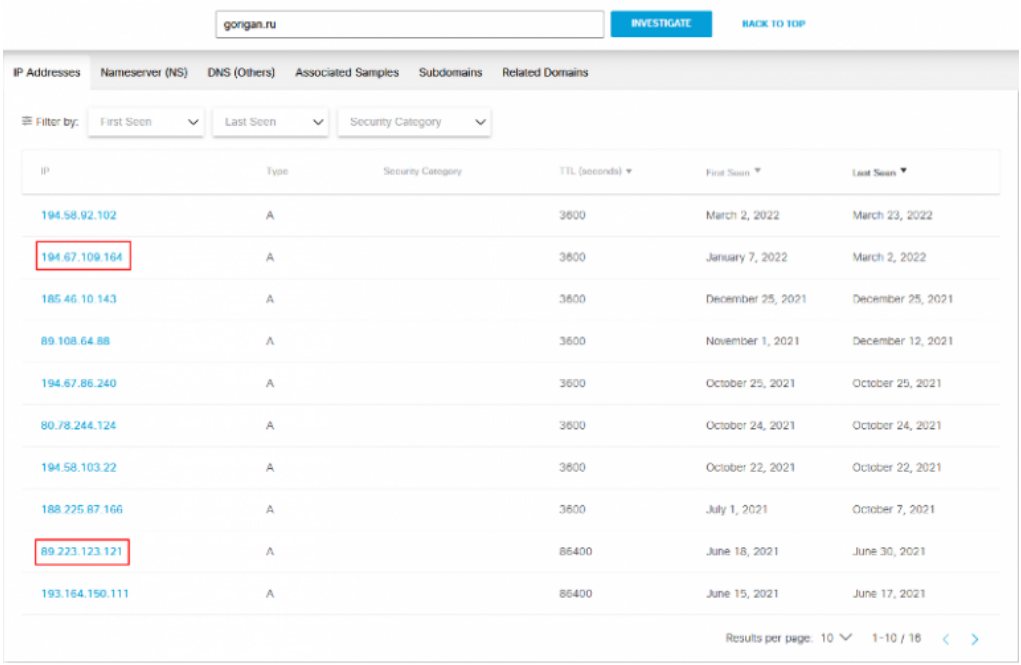
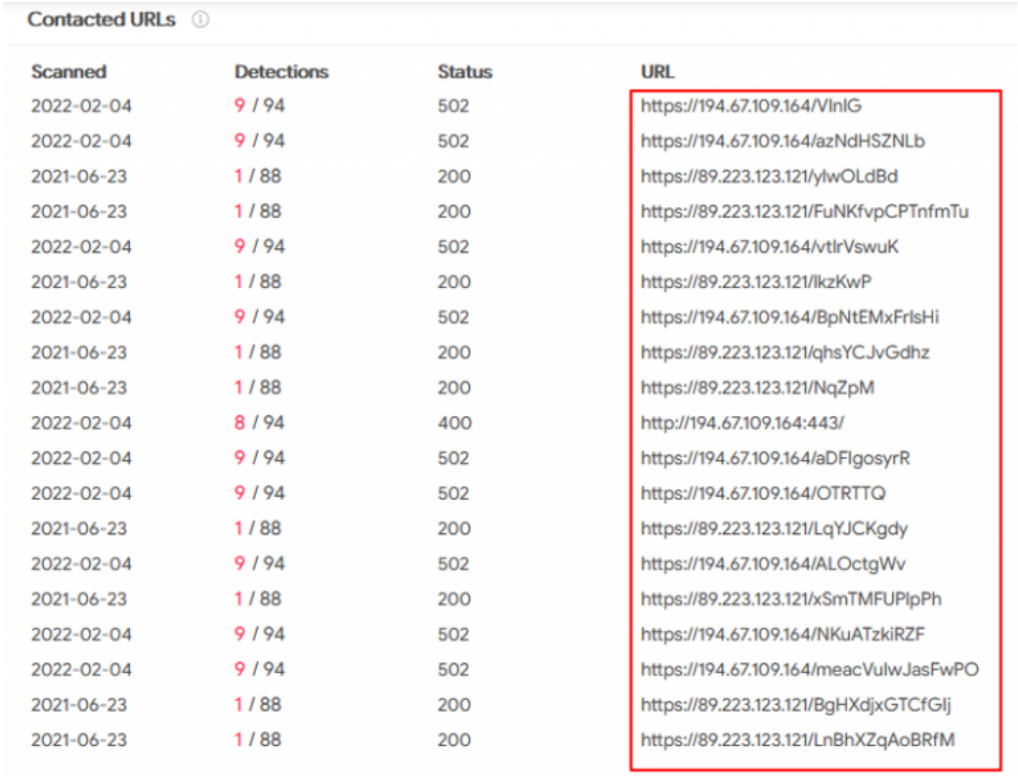


Figure 1: IP address resolutions of gorigan[.]ru



Contacted URLs

Scanned	Detections	Status	URL
2022-02-04	9 / 94	502	https://194.67.109.164/VlnlG
2022-02-04	9 / 94	502	https://194.67.109.164/azNdHSZNLb
2021-06-23	1 / 88	200	https://89.223.123.121/ylwOLdBd
2021-06-23	1 / 88	200	https://89.223.123.121/FuNKfvpCPTnfmTu
2022-02-04	9 / 94	502	https://194.67.109.164/vtlrVswuK
2021-06-23	1 / 88	200	https://89.223.123.121/lkzKwP
2022-02-04	9 / 94	502	https://194.67.109.164/BpNtEMxFrlsHi
2021-06-23	1 / 88	200	https://89.223.123.121/qhsYCJvGdhz
2021-06-23	1 / 88	200	https://89.223.123.121/NqZpM
2022-02-04	8 / 94	400	http://194.67.109.164:443/
2022-02-04	9 / 94	502	https://194.67.109.164/aDFlgosyrR
2022-02-04	9 / 94	502	https://194.67.109.164/OTRTTQ
2021-06-23	1 / 88	200	https://89.223.123.121/LqYJCKgdy
2022-02-04	9 / 94	502	https://194.67.109.164/ALOctgWv
2021-06-23	1 / 88	200	https://89.223.123.121/xSmTMFUPlpPh
2022-02-04	9 / 94	502	https://194.67.109.164/NKuATzkiRZF
2022-02-04	9 / 94	502	https://194.67.109.164/meacVulwJasFwPO
2021-06-23	1 / 88	200	https://89.223.123.121/BgHXdjxGTCfGlj
2021-06-23	1 / 88	200	https://89.223.123.121/LnBhXZqAoBRfM

Figure 2: URL connections to resolved IP addresses (source: Virustotal)

Detecting Gamaredon Activity with Global Threat Alerts

In Cisco Global Threat Alerts, we are tracking the Gamaredon group under the **Gamaredon Activity** threat object. The threat description is enriched with MITRE references (see Figure 3).

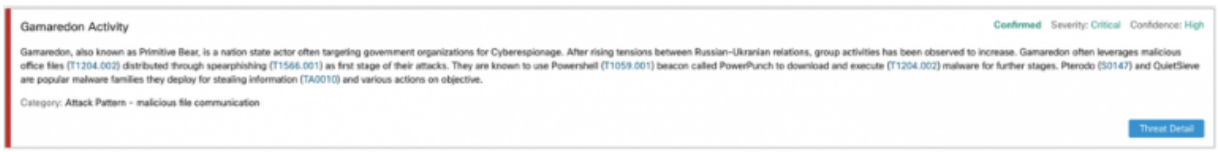


Figure 3: Threat description of Gamaredon activity, including MITRE techniques and tactics (source: Cisco Global Threat Alerts)

Figure 4 shows a detection sample of Gamaredon activity. Observe that the infected device attempted to communicate with the domains alacritas[.]ru, goloser[.]ru, and libellus[.]ru, which seemed to be sinkholed to the OpenDNS IP address of 146.112.61.[.]107.

Figure 4: Gamaredon group detection example (source: Cisco Global Threat Alerts)

Conclusion

We've walked through the steps of producing intelligence from information we've collected. We began our analysis with an unattributed list of network IoC's and were able to identify unique patterns in their metadata. Then, we pivoted to endpoint IoC's and attributed domains to malware families. Next, we showed how we turned it into a detection of the Gamaredon group displayed in the Cisco Global Threat Alerts portal.

For your convenience, here's a summary of the intelligence we developed in this blog post:

Aliases	Primitive Bear, Shuckworm, ACTINIUM
Type	Threat Actor
Originating From	Russia
Targets	Ukranian State Organizations
Malware used	Pterodo, Groooboor
File Type	Macro enabled office files, Win32 Exe, VBA
TLD's used	.online, .xyz, .ru, .site, .space
ASN's used	REG.RU, Ltd, TimeWeb Ltd., EuroByte LLC, AS-CHOOPA, LLC Baxet, System Service Ltd.

References

[1] Cyber Group Tracker: https://cyberknow.medium.com/update-10-2022-russia-ukraine-war-cyber-group-tracker-march-20-d667afd5afff

[2] Conti ransomware's internal chats leaked after siding with Russia: https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/

[3] Hackers sound call to arms with digital weapon aimed at Russian websites: https://cybernews.com/news/hackers-sound-call-to-arms-with-digital-weapon-aimed-at-russian-websites/

[4] Threat advisory: Cybercriminals compromise users with malware disguised as pro-Ukraine cyber tools: https://blog.talosintelligence.com/2022/03/threat-advisory-cybercriminals.html

[5] Ukraine-Cyber-Operations: https://github.com/curated-intel/Ukraine-Cyber-Operations

[6] What You Need to Know About Russian Cyber Escalation in Ukraine: https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/

[7] Gamaredon: https://attack.mitre.org/groups/G0047/

[8] Pteranodon: https://attack.mitre.org/software/S0147/

[9] Sandworm: https://attack.mitre.org/groups/G0034/

[10] Threat Advisory: Cyclops Blink: https://blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html

[11] Wizard Spider: https://attack.mitre.org/groups/G0102/

[12] Cobalt Strike: https://attack.mitre.org/software/S0154

[13] Emotet: https://attack.mitre.org/software/S0367

[14] Conti: https://attack.mitre.org/software/S0575

[15] Ryuk: https://attack.mitre.org/software/S0446

[16] TrickBot: https://attack.mitre.org/software/S0446

[17] Technical Report Gamaredon/Armageddon group: https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf

[18] ACTINIUM targets Ukrainian organizations: https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
