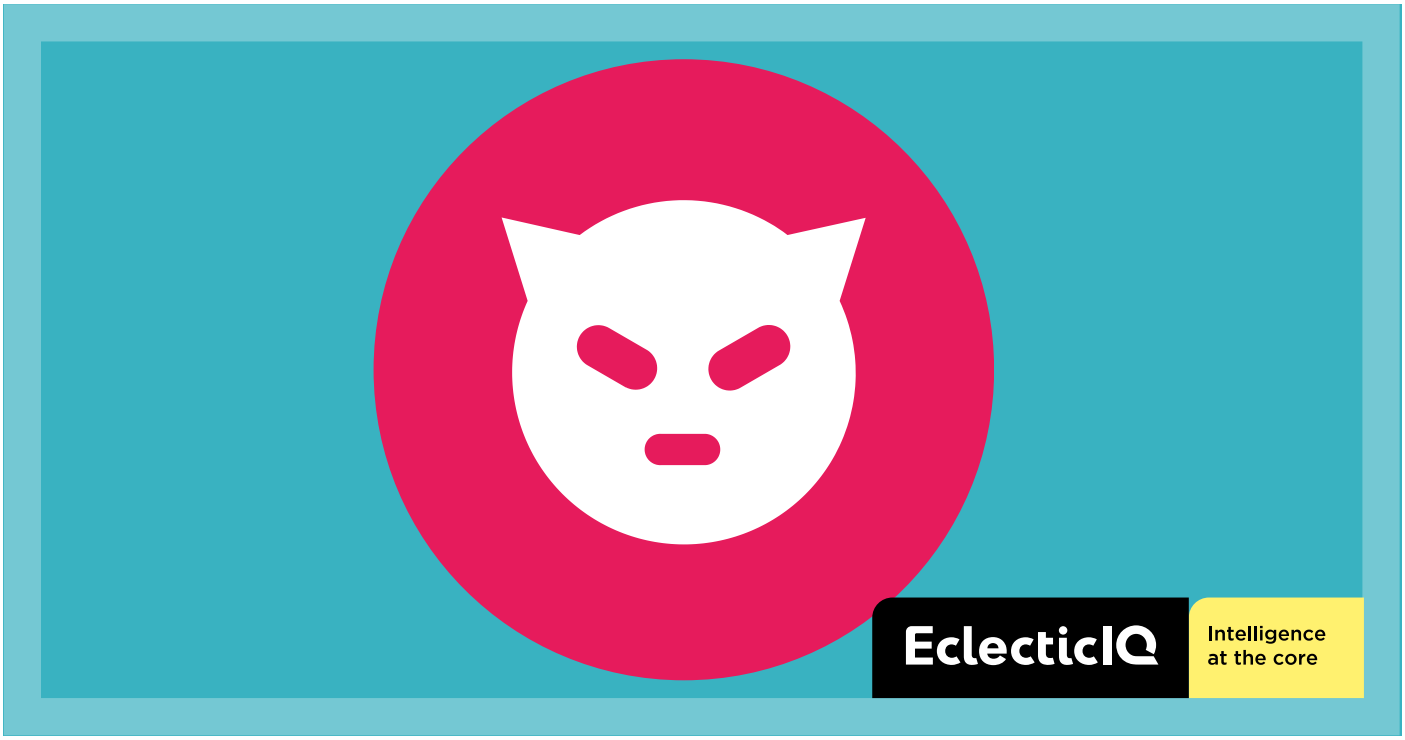
Exposed Web Panel Reveals Gamaredon Group's Automated Spear Phishing Campaigns

Arda Büyükkaya – April 17, 2023 (Updated on April 18, 2023)



Executive Summary

On February 09, 2023, EclecticIQ analysts identified a spear phishing campaign targeting Ukrainian government entities like the Foreign Intelligence Service of Ukraine (SZRU) and Security Service of Ukraine (SSU). Analysts identified a publicly exposed Simple Mail Transfer Protocol (SMTP) server and assess with high confidence that the threat actor used the SMTP server to craft and deliver phishing emails.

The SMTP server contained a web panel designed to create and distribute spear phishing emails. It enables the email to have a malicious attachment and leverages email spoofing techniques to make it appear from a legitimate source.

Observed adversary tactics, techniques, and procedures (TTPs), victimology, and infrastructure found in the SMTP server configuration overlap with previously identified Gamaredon activity.

Key Judgments

Gamaredon APT group is believed to be a Russian State-backed threat group linked to the Federal Security Service (FSB). Gamaredon is known for its cyberespionage activities, primarily targeting

Ukrainian government entities. The group uses spear phishing emails and social engineering lures as a primary tactic.

The threat actor used a generic web panel to craft and send phishing emails against Ukrainian government entities. This allowed the actor to automate the malware delivery process against specific targets entered by the attackers in the email recipient section of the panel's user interface.

Pivoted IP addresses overlap with previously reported Gamaredon activity (8).

Web Panel Uncovered as Source of Phishing Attacks

EclecticIQ analysts discovered a publicly facing SMTP server 194[.]180[.]191[.]56 used in a spear phishing campaign against Ukrainian government entities in February 2023. The exposed SMTP server hosts a web panel for crafting and delivering spear phishing emails. Analysts assess with high confidence that the threat actor used this infrastructure to send large number of spear phishing emails automatically. Figure 1 shows two example phishing emails sent from the server:

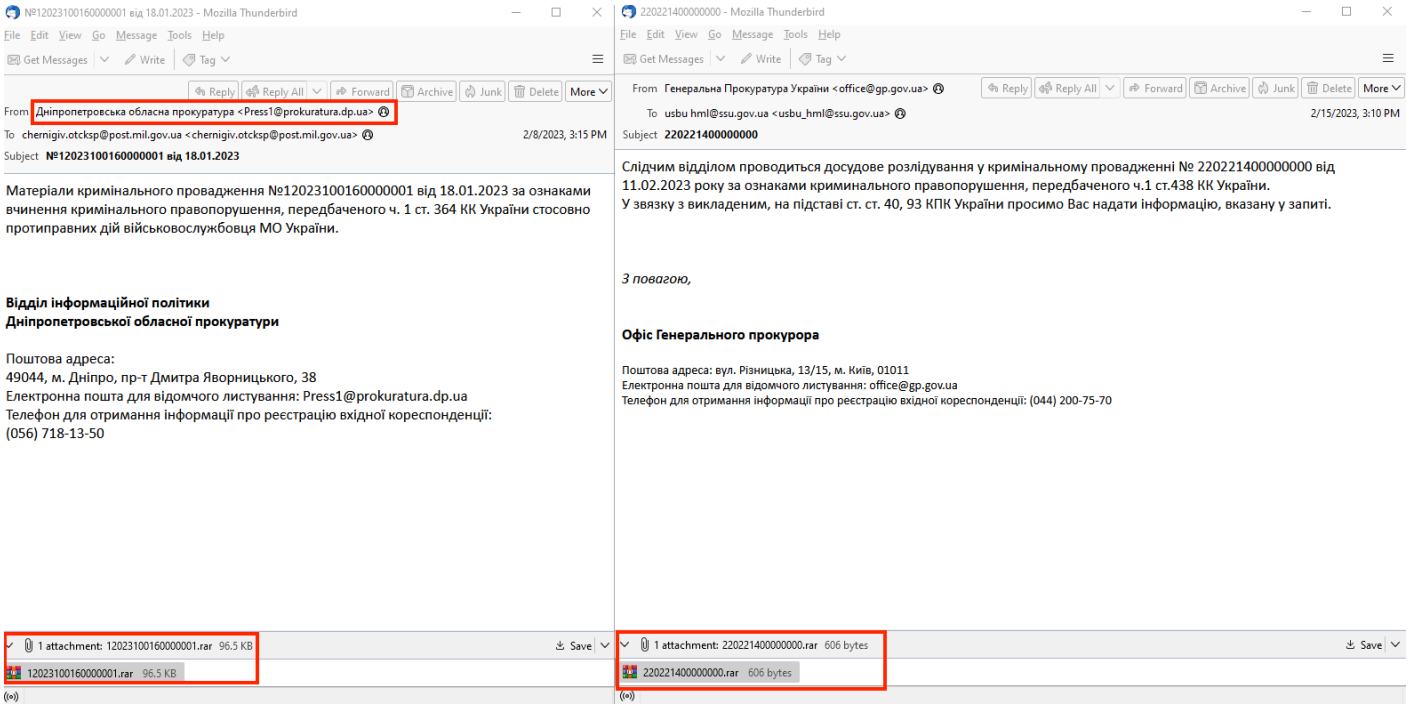


Figure 1 - Example of phishing emails with malicious attachment sent in in February 2023.

EclecticIQ analysts identified these two different spear-phishing emails sent from 194[.]180[.]191[.]56. Both of these emails contain a RAR archive file as an attachment, which are used to deliver the initial malware. Figures 2 and 3 showed two different malware execution flows, sent on Wed, 15 Feb 2023 17:10:18 +0200 and Wed, 08 Feb 2023 17:15:44 which are identical to previous Gamaredon campaigns (1).

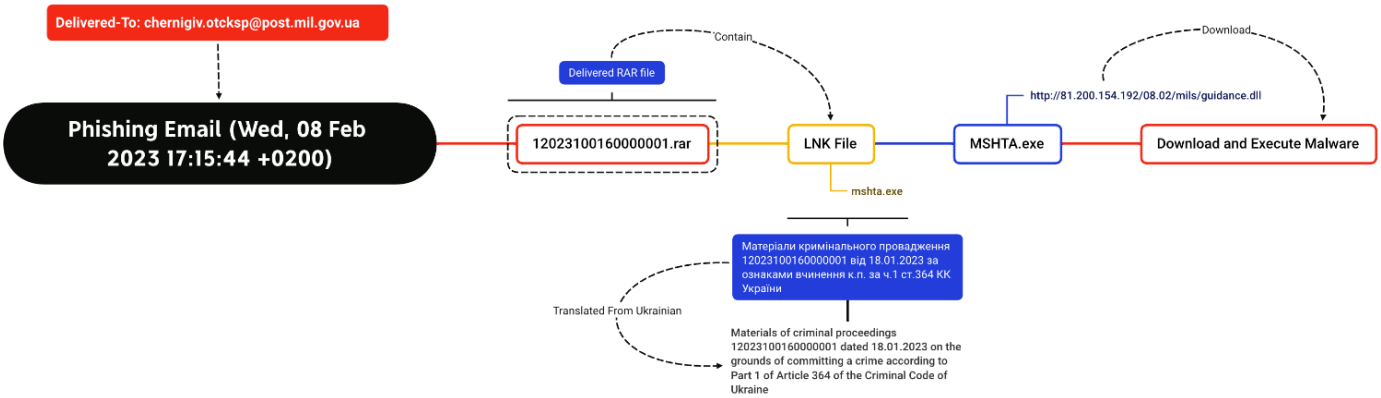


Figure 2 - Spear phishing email sent on Wednesday, 15 February 2023.

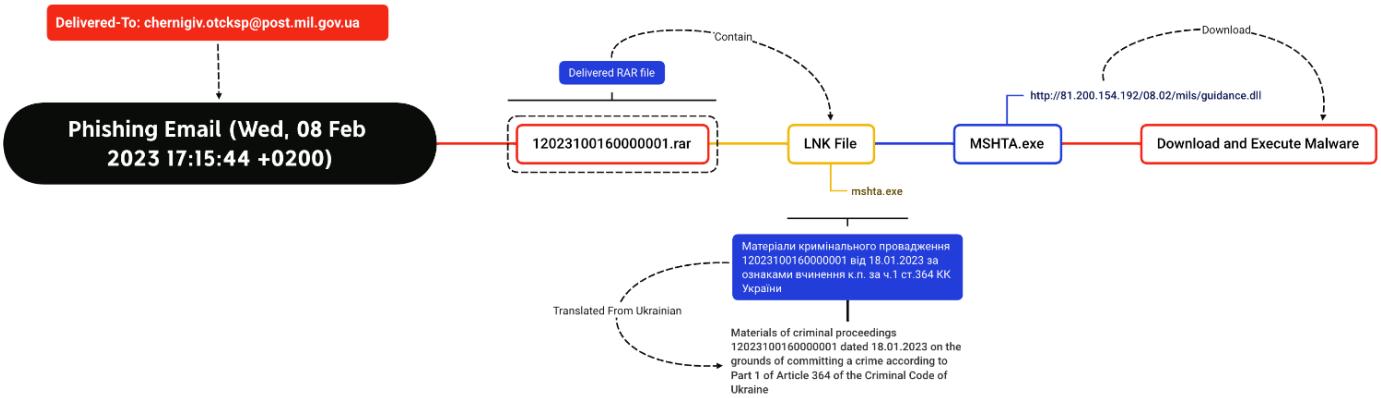


Figure 3 - Spear phishing email sent it on Wednesday, 8 February 2023.

Figure 4 shows the origin of the phishing email and spoofed email address:

```
Return-Path: <pivn-kr@prokuratura.dp.ua>
Delivered-To: chernigiv.otcksp@post.mil.gov.ua
Received: from post.mil.gov.ua
    by post with LMTP
    id KHxHCqC842O/Hy0AY18K5Q
    (envelope-from <pivn-kr@prokuratura.dp.ua>)
    for <chernigiv.otcksp@post.mil.gov.ua>; Wed, 08 Feb 2023 17:15:44 +0200
Received: from [127.0.0.1] ([127.0.0.1:43728] helo=smtp-injection-worker)
    by prd07-euw1-05 (envelope-from <pivn-kr@prokuratura.dp.ua>)
    (ecelerity 4.3.1.999 r(:)) with ESMTPS (cipher=ECDHE-RSA-AES128-GCM-SHA256)
    id 41/E3-11317-F9CB3E36; Wed, 08 Feb 2023 15:15:43 +000015:15:40 +0000 (UTC)
Received: from [194.180.191.56] (port=37552 helo=ousyaxmchj)
    by skm191.hostsila.org with esmtpa (Exim 4.95)
    (envelope-from <pivn-kr@prokuratura.dp.ua>)
    id 1pPmAd-007Kxf-V5
    for chernigiv.otcksp@post.mil.gov.ua;
```

Figure 4 - Source of phishing email.

The server had port 80 open for use by the threat actor for crafting spear phishing emails via a simple user interface seen in figure 5.

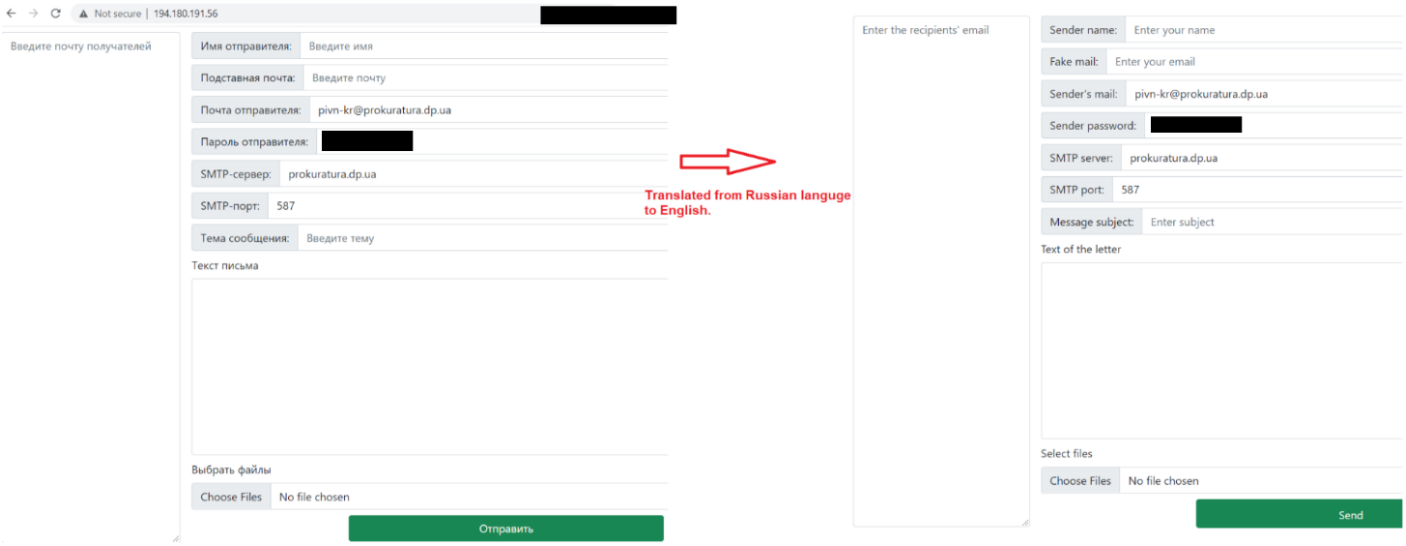


Figure 5 - Web panel translated from Russian to English.

The web panel allowed the threat actor to send emails using the hardcoded sender address pivn-kr@prokuratura[.]dp[.]ua. EclecticIQ analysts identified the same email address in a recent phishing email campaign sent to a Ukrainian military address on February 9, 2023 (5), indicating that the exposed panel was very likely used for malware delivery.

.htaccess Reveals Additional Adversary Infrastructure

EclecticIQ analysts identified that the “.htaccess” file on the exposed SMTP server was misconfigured. The ”.htaccess” file is a directory-level configuration to limit access to a web server from trusted IP addresses only. According to the Apache documentation, users must insert all IP filters inside the " <RequireAll>" tag (7). However, this tag was missing in the configuration used by threat actor.

Analysts identified five IP addresses in the “.htaccess” file (figure 6):

- 109[.]200[.]159[.]40
- 151[.]236[.]30[.]50
- 109[.]200[.]159[.]59
- 109[.]200[.]159[.]46
- 192[.]121[.]87[.]11

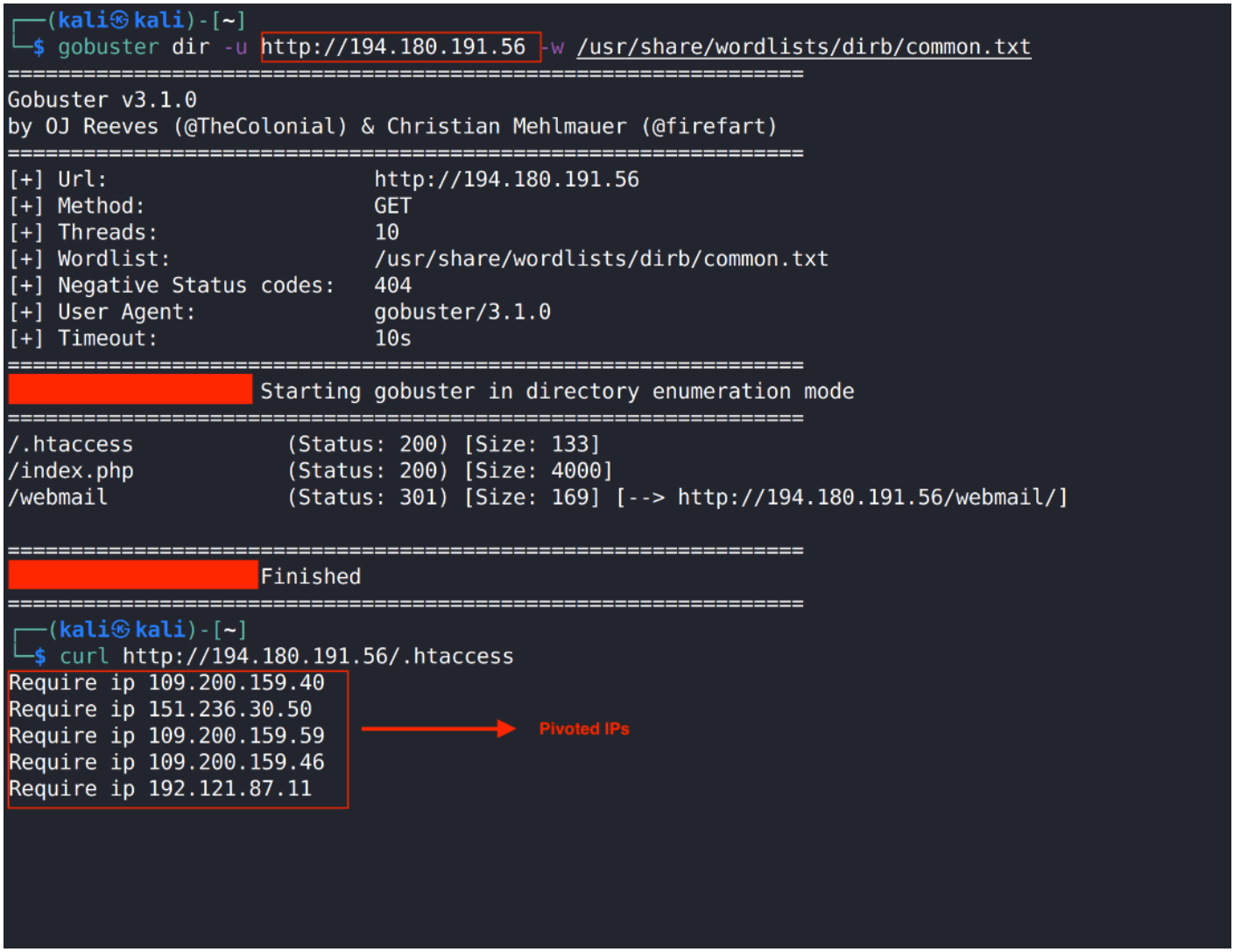


Figure 6 – Reconnaissance with gobuster (6) and pivoting.

The majority of the pivoted IP addresses are located in Moscow, Russia from the same server provider, Crelcom LLC (AS 6789). WHOIS records show that one of the IP addresses - 109[.]200[.]159[.]46 - was registered under the name Michael Tishin. The same name is also listed as registrant for another IP - 109[.]200[.]159[.]54. This IP was attributed to Gamaredon by BlackBerry on January 19, 2023 (8).

TTPs, Victimology and Infrastructure Overlaps with Gamaredon Activity

The adversary TTPs and victimology overlap with Gamaredon activity previously reported by EclecticIQ and other researchers starting in 2020 (1).

EclecticIQ analysts identified one IP address 109[.]200[.]159[.]59 in the ".htaccess" file that links to a spear phishing email submitted to VirusTotal on November 20, 2020. In May 2022, Cisco reported the campaign and attributed the activity to Gamaredon (2, 4).

Figure 7 shows the connection between the pivoted IP addresses and malicious files uploaded to VirusTotal. The IP address links to a spear phishing email with a malicious attachment. The attachments exploit CVE-2017-0199, a Microsoft Office remote code execution vulnerability in Windows.

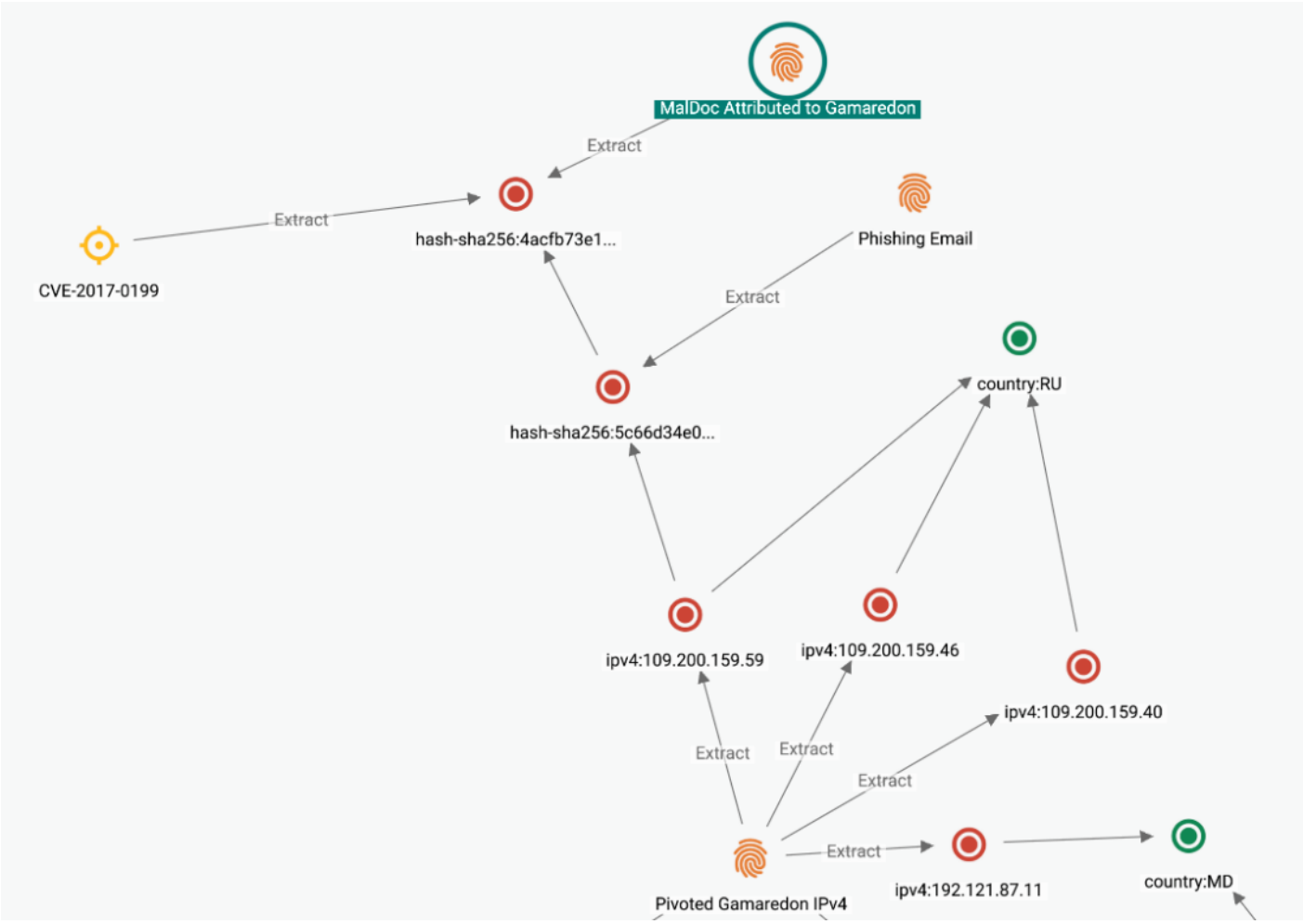


Figure 7 – Link analysis for 109[.]200[.]159[.]59.

Figure 8 shows that spear phishing email was sent to the Security Service of Ukraine (SSU) on November 19, 2020. It contained a malicious Word document attachment used for malware delivery. The email sender section was spoofed by threat actors to make the email look legitimate.

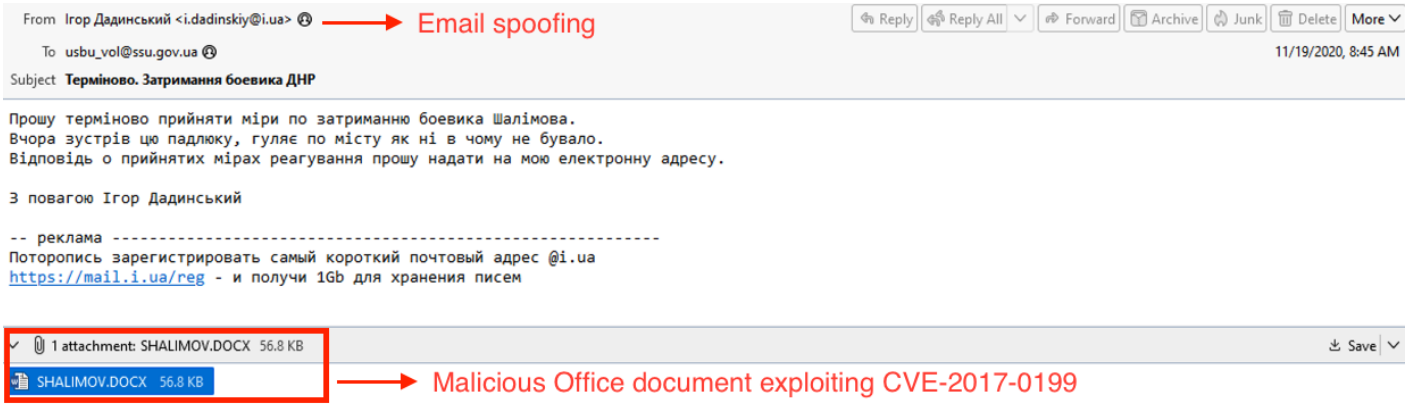


Figure 8 – Content of the phishing email.

Figure 9 displays the metadata of the spear phishing email. The "X-Sender-IP" field in the metadata reveals the IP address 109[.]200[.]159[.]59 of the sender. This IP address does not match the domain name (i.ua) in the “From” field, proving it is a spoofed email.

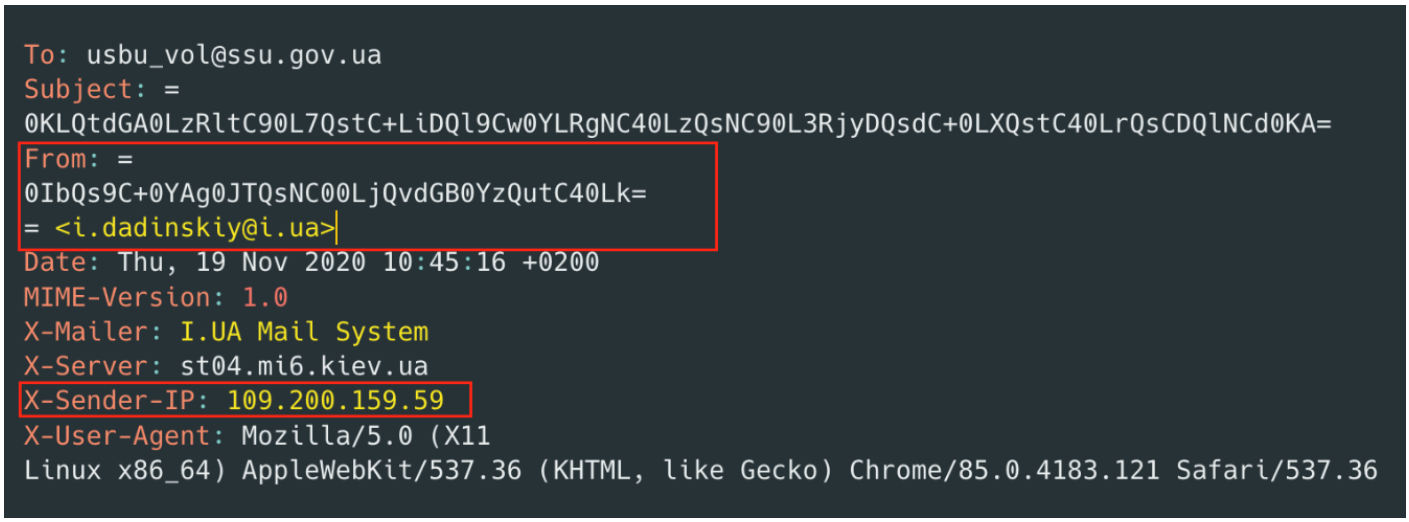


Figure 9 – Metadata section inside phishing email.

Once a victim opens the delivered malicious Word document, it will exploit CVE-2017-0199. If the exploitation is successful, then it will download a second-stage malware from the domain erythrocephala[.]online, which has been attributed to Gamaredon.

Outlook

EclecticIQ analysts assess with high confidence that Russian government-linked APTs will continue to use social engineering tactics during cyberattacks against Ukraine. Additionally, they are expected to increasingly target NATO partners due to NATO's support of Ukraine during the Russian war.

It is very likely that the threat actor will modify their TTPs to avoid detection that will increase their chances of success, especially during the malware delivery stage.

Protections and Mitigations

- **Regularly educate employees**: Phishing attacks often rely on social engineering to trick recipients into divulging sensitive information or performing a certain action. By educating employees on how to recognize and avoid phishing emails, you can reduce the risk of a successful attack.
- **Implement SPF, DKIM, and DMARC to prevent email spoofing**: SPF specifies authorized IP addresses and domains, DKIM signs outgoing emails with a digital signature, and DMARC builds upon SPF and DKIM to provide comprehensive protection by allowing domain owners to specify handling for failed checks.
- **Install updates**: Microsoft released patches and updates to fix vulnerabilities such as CVE-2017-0199. Users must install these patches and updates when they are released to minimize exploitation.
- **Implement Content Filtering**: Content filtering can be used to block specific files from being downloaded or received by email. This can prevent users from unintentionally opening and executing malicious files.