Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity

Stories

The latest cybersecurity trends, best practices,
security vulnerabilities, and more

By Daksh Kapur, Tomer Shloman, Robert Venal and John Fokker · January 24, 2023

Figure 1

It has been almost a year since Russia invaded Ukraine in a major escalation of the Russo-Ukrainian War, which began in 2014. It has caused Europe's largest refugee crisis since World War II. The war is not just occurring on land but also through technology systems: Ukraine public, energy, media, financial, business and non-profit sectors have suffered the most through repeated, targeted cyberattacks. Since Feb 2022, cyberattacks have undermined the distribution of medicines, food and relief supplies. Their impact has ranged from preventing access to basic services to data theft and disinformation. In our previous blog we described the different attacks against Ukraine that we observed through our telemetry.

Our team has been following the cyberthreat landscape closely, supporting our global government and enterprise customers with the latest threat intelligence and indicators. In this blog, we outline our latest findings around cyberactivity targeting Ukraine. From malicious email and URLs to nation-state backed use of malware, cyberactivity continues to accompany kinetic military activity and social discontent.

Malicious email

A year later, and the Trellix Advanced Research Center team has noticed a 20-fold increase in email based cyberattacks on Ukraine's public and private sectors. Our email security researchers observed a surge of attacks in the third week of November '22 which remained consistently high until they descended at the end of December '22.

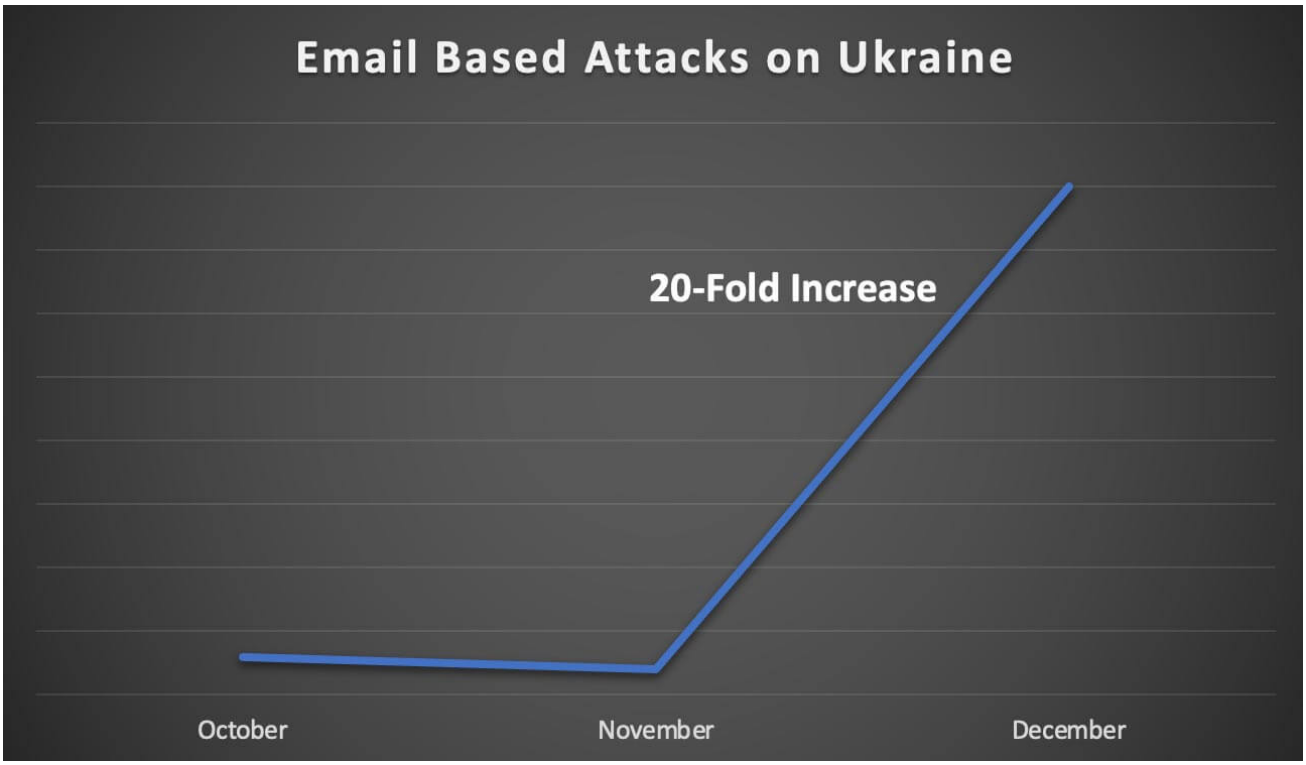


Figure 2 – Email based Attacks on Ukraine in 2022

The majority of these attacks were found to be aimed towards subdomains of "gov.ua" website which is the parent domain for Ukrainian government and military sites. The most popular attacks were attachment-based in which emails with minimal body content along with an attachment were sent to the victim. The subject is usually something to catch interest like "References regarding receivables and payables," "Please urgently submit an application for a work permit for January 2022."

Different types of attachments were used to deliver malware. Some examples include xlsx, shtml, doc, xlsm, jar, lnk and cmg, of which xlsm was the most prevalent. The large majority of the observed malicious emails directed at the Ukrainian government had a nefarious sender, based on the analysis of the malicious attachments we believe with a high level of confidence that these can be attributed to the state sponsored group Gamaredon.

Email campaigns

Trellix Advanced Research Center researchers found different styles of campaigns utilized to target Ukrainian websites:

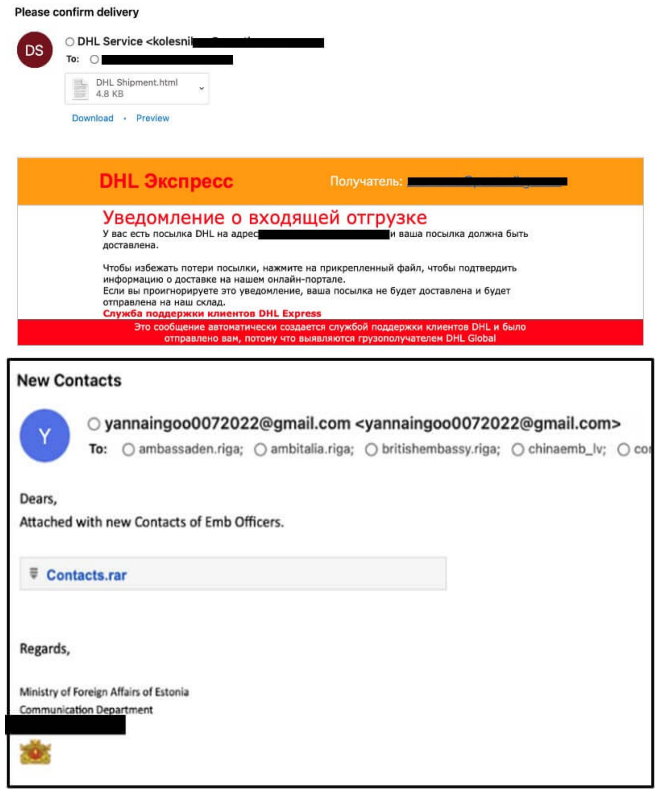
Sample 1: The email is a fake inbound Shipment Notification containing a html file opening which redirects the victim to a customized phishing page.

Sample 2: An email pretending to be from the “Accounts Team” that contains a malicious attachment masqueraded as an invoice

Sample 3: An email pretending to be from the Ministry of Foreign Affairs of Estonia looking to share contacts of embassy officers, and containing a link redirecting the user to a Google drive link containing a malicious file

Sample 4: An email pretending to be from “Ministry of Defense of Ukraine” and contains a compressed archive as an attachment, the email also utilizes the name of a logistic company, DNI Pro LLC which actively works in Ukraine. The archive is used to deliver malware to the victim.

Sample 5: A fake notification email from an Administrator for mil.gov.ua notifying the victim of issues with their mailbox that require verification to resolve, and containing a link that redirects the user to a malicious website



FW: Sales Invoice - 392692 and 392682

AR ○ Accounts Receivable [redacted]

To: ○ [redacted]

Sales Invoice - 3926...
0.4 KB

Download • Preview

Good Afternoon,

Please find attached your current invoice for your review.

Thank you.

Best Regards,

Unical Aviation, Inc.
Accounts Receivable Dept.
Direct: [redacted]
Fax: [redacted]

Виявлено фішингове повідомлення

B ○ Броварський РТЦК та СП <[redacted]

To: ○ [redacted]

розпорядження.rar
19.3 KB

Download • Preview

--- Повідомлення, що пересилається ---
Від кого: "МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ" <[redacted]
Кому: <[redacted]
Тема: Передати електронною поштою АСУ "Дніпро" (згідно розрахунку розсилки)
Дата: 27 грудня 2022, 14:10:41

--
З повагою,

ПРИЙМАЛЬНА ДЕРЖАВНОГО СЕКРЕТАРЯ
МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ
E-mail: [redacted]

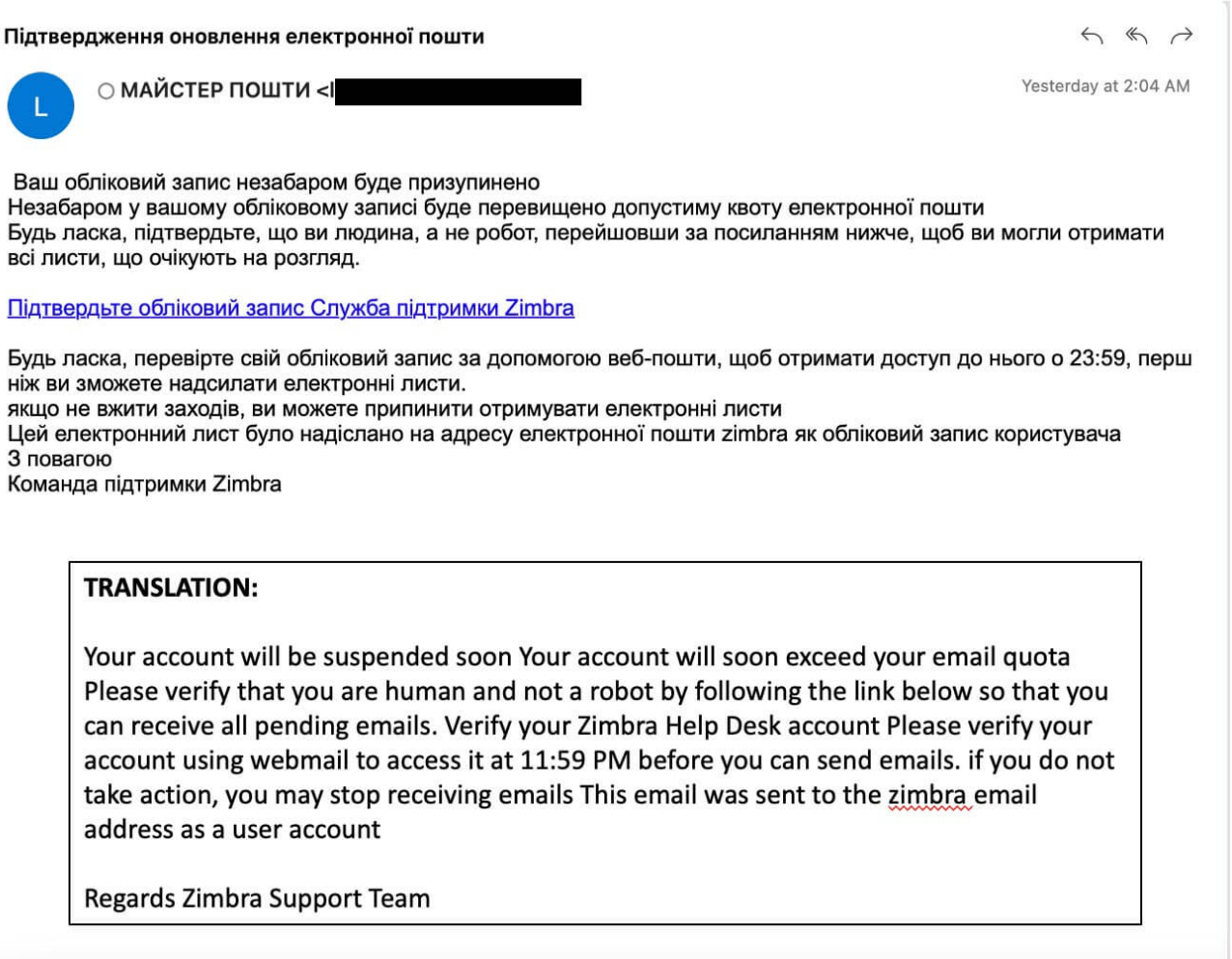


Figure 3 - Malicious Emails targeting Ukraine

Malicious URLs

The following are some of the malicious web pages being utilized to target Ukraine which were found by Trellix Advanced Research Center's email researchers:

- Customized pages that appear to be genuine and look like the legitimate pages they spoof make it difficult for the victim to recognize any suspicious activity
- Capitalizing on user's sense of urgency like by presenting a blurry document as a background of the phishing page, the document is designed to look important hence capitalizing on the feeling of urgency to convince victim to log in.
- The pages also make use of a combination of techniques to attempt to evade detection by security products and make it harder to analyze by security professionals.

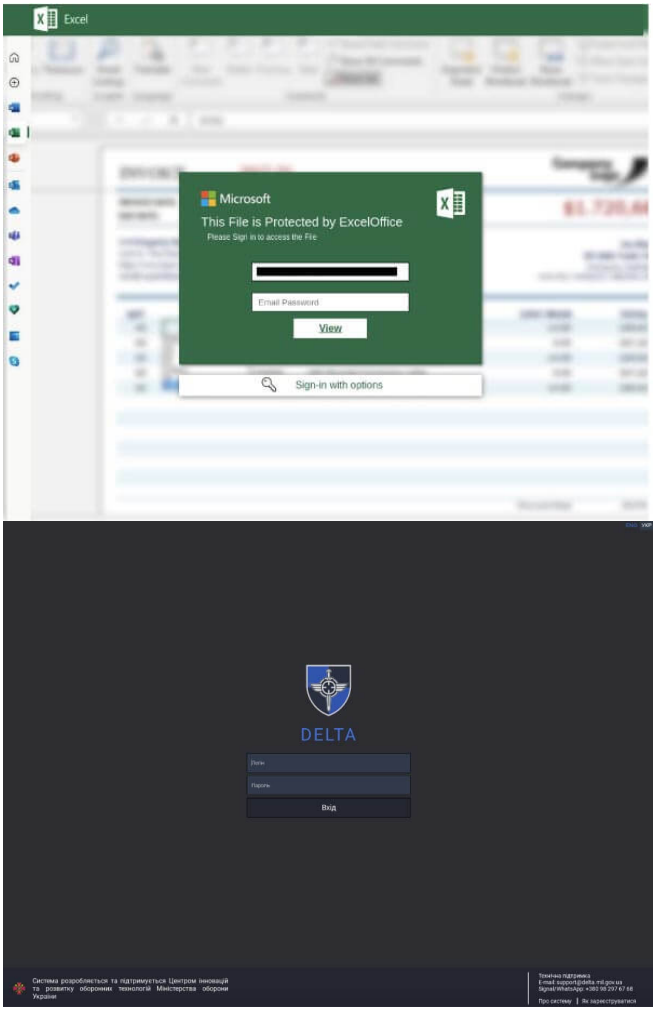


Figure 4 - Malicious URLs targeting Ukraine

Malware and suspicious behavior

Trellix Advanced Research Center telemetry has identified several malware families and observed suspicious behavior targeting Ukraine organizations. The following are some of the malware families and behaviors observed by our researchers:

- **Garmaredon:** Gamaredon – A Russian APT group and one of the most active State sponsored groups targeting Ukraine. The name Gamaredon Group comes from a misspelling of the word "Armageddon", which was detected in the adversary's early campaigns. Trellix researchers observed three different styles of malware related to Garmaredon.
    - The first which contained malicious LNK downloaders contained in archive files of various formats. These are trojans that abuse the Windows MSHTA utility to download further stages of malware.
    - The second was doc files using template injection attacks. This type of attack is a Word document with fake template references to external malware payloads.
    - The third were XLL downloaders. These are trojanized Excel add-in DLLs that are programmed to instead download and install further malware.
- **H-Worm:** also known as Houdini Rat is a Visual Basic Script based Remote Access Trojan (RAT) first spotted in 2013. Command and Control infrastructure is shared with other malware families such as NjW0rm, njRat, XtremeRAT, and PoisonIvy. The RAT contains various capabilities including stealing system information, capturing screenshots, logging keystrokes, viewing the webcam, deleting files, and uninstalling itself. H-Worm was deployed in targeted attacks against the international energy industry. We have also seen it used in a wider context for run-of-the-mill attacks executed through spammed email attachments and malicious links.
- **Formbook:** An info stealer malware used to steal several types of data from infected systems, including credentials cached in web browsers, screenshots, and keystrokes. It can also act as a downloader, enabling it to download and execute additional malicious files.
- **Remcos:** A Remote Access Software used to remotely control computers, which once installed, opens a backdoor on the computer, granting full access to the remote user.
- **Andromeda:** A commodity trojan developed in 2011 currently targeting Ukraine public sector networks. This re-emergence of Andromeda was previously reported by Mandiant, and Trellix can confirm this Andromeda activity.
- **Potentially Unwanted Program (PuP) detections:** From October 2022 till January 2023, we observed an abnormally large amount of PUP detections in Ukraine linked to a single software activation program aimed at activating Adobe. However, this PuP was actually malware aimed at creating a backdoor on the infected system. The usage of PuPs and pirated license activators is something we continue to observe in our telemetry. We strongly discourage this behaviour as it increases the risk of serious malware infections.

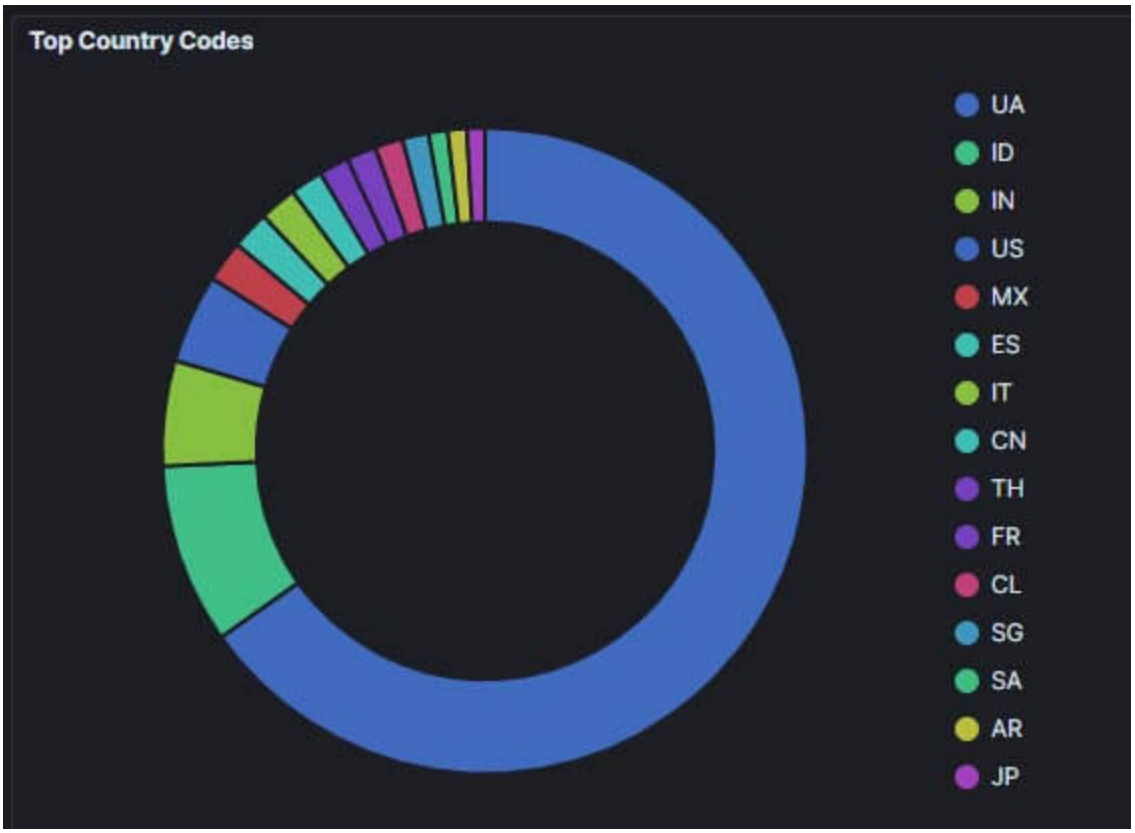


Figure 5 Abnormal amount of PUP detections from Ukraine

- **CVE-2021-3438:** We have observed multiple privilege escalation attempts at a financial Institution where the threat actor attempted to launch an exploit for a known HP printer vulnerability (CVE-2021-3438) via Rundll32.
- **Suspected MSIEXEC.exe activity:** Our researchers observed suspicious behavior where msiexec.exe was spawned from an Excel file and attempted to download a binary from a potentially compromised Qnap NAS device exposed to the Internet. Leveraging MSIEXEC.EXE is a common techniques, however, have observed this specific behavior previously in a Raspberry Robin campaign as well as a older Gamaredon campaign. More definitive attribution wasn't possible as the final payload was no longer available for additional analysis.

Indicators of compromise

The following link contains examples of malicious URLs, binaries and email addresses used in the campaigns being carried against Ukraine.

Trellix security protection

Trellix provides reliable detection from such campaigns by preventing emails from ever reaching your system. In addition, Trellix also detects campaigns on other levels like network, URL and binary to provide complete protection to our customers.

The following is a subset of the Trellix Security detections that have been observed for the malware in these campaigns:

Email Based Detections -

- FE_EMAIL_PASSWORD_RESET_PHISH_1
- FE_Trojan_HTM_Phish_198.FEC2
- FEC_Trojan_JS_Generic_14
- FEC_Dropper_HTML_Generic_18

Endpoint Based Detections -

- APT.Gamaredon.DNS
- Worm.Houdini
- FE_Backdoor_Win32_REMCOS_2
- Trojan.Formbook
- FE_Worm_Win32_Andromeda

Conclusion

As the Ukraine-Russia war continues, the cyber-attacks on Ukraine energy, government and transportation, infrastructure, financial sector etc. are going on consistently. In times of such panic and unrest, the attackers aim to capitalize on the distraction and stress of the victims to successfully exploit them. As the attacks continue, we suggest everyone stay vigilant. Government and defense personnel are advised to stay extra-careful as they would be the most promising targets for the attacks.

To review previous research on threat activity targeting Ukraine, check out our Trellix Advanced Research Center's previous blogs on Wiper malware and the evolution of Russian cyber activity targeting Ukraine.

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers.

Zero spam. Unsubscribe at any time.