TIPPER_2022_003

Bitdefender®

Managed Detection and Response

Ukraine Conflict

February 28, 2022

www.bitdefender.com

Details

Bitdefender has been monitoring the Ukraine conflict closely to ensure our customers are protected. As a Bitdefender MDR client, we take your security seriously and are always looking for malicious activity from a wide range of threat actors.

The MDR service uses the customer questionnaire, threat intelligence feeds, and open-source intelligence to build a customer-specific threat landscape, which allows us to continuously and smartly monitor cyber threats. In turn, this leads to relevant actions like hunt packages, which allows our MDR analysts to search for specific system behavior and indicators in your environment. Our research team is constantly searching for new indicators, which are built into signatures that allow us to stay abreast of the most current threats.

Our Current Perspective

The current focus of the highest risk threat activity is on Ukraine. Recent assessments indicate the likelihood of being targeted by a malicious actor in the coming days and weeks will not be the same for every organization. That is, while there is always a chance of coming under attack from a nation-state APT, the daily risks and most likely threats still arise from cybercrime in general, and technical threats such as ransomware. In Bitdefender's most recent blog, we discussed several tiers of organizational factors that tie into consideration of risk.

While below is not an all-encompassing list of factors to consider, your threat model may change over time as the situation develops. You may only carry a risk of an indirect attack, or, depending on your business, face increasing risks over time. We recommend looking at your risk profile holistically, considering the points we've brought up here, as well as your own implementation of best practices and security posture.

Here are some factors to think about how the current threat landscape might change for you specifically:

- Do you have US/EU government contracts?
- Are you providing direct assistance to the government or armed forced of Ukraine or any EU/NATO countries?
- Are you associated with any businesses or governments currently involved in sanctions?
- Does your business have information that would be of high value to a motivated nation-state, such as wartime operational or contingency planning, technical military data, or similar sensitive defense information?
- Do you have any cleared defense contractors?
- Do you control financial services or assets that, if targeted, could impact the US or EU governments?
- Do you control or provide services to the Energy Sector, or businesses related to critical national infrastructure?

- Are you actively part of a humanitarian assistance organization, involved in resettlement of displaced people, or otherwise directly assisting the people of Ukraine? This doesn't mean donations to the cause; this would imply directly involved in boots-on-ground assistance to refugees.

What We Expect Next

As the invasion continues, we expect malicious cyber efforts to focus on Ukraine most heavily followed by countries that have imposed sanctions. This will most likely include private or public sector companies that meet the criteria of the questions above, but as we saw with the NotPetya attacks in 2017, there is always the chance for unintended victims.

Increased rhetoric from various governments as sanctions increase will likely cause further responses from APTs and some cybercriminal groups, who may act as proxies. During the first few days of the war, several malicious actors have pledged a willingness to target organizations who undertake offensive cyber operations. There have also been reports of hacktivist activity from groups such as Anonymous, which will likely continue to varying degrees of success, and direct recruitment efforts to bring more hackers to Ukraine's defense.

Phishing and social engineering will be the most likely to affect everyone during this operation. Threat actors such as the notorious Fancy Bear and similar APTs are proficient with phishing and malware, as well as with techniques that "live off the land," which use standard system tools, such as PowerShell, to perform reconnaissance, lateral movement, privilege escalation, and exfiltration, among other techniques. Some of these actors recently have taken advantage of public cloud infrastructure, including compromised cloud storage or sites such as Discord, to host malware or act as command & control (C2) infrastructure. This is in addition to previous techniques of using spoofed domains designed to appear legitimate at first glance.

Bottom line, users should beware of any emails that provoke sensationalism or urgency. Users should also exercise extreme caution when investigating links within emails or downloading attachments, especially from unfamiliar senders.

Finally, disinformation and information warfare campaigns will likely continue to be problematic for media reporting and other public information outlets, such as social media. These campaigns may work in concert with phishing and social engineering, or contain aspects of these techniques, e.g., "clickbait." Since this is the second most likely to directly affect you or your users, we recommend using caution when reposting or sharing information, and vetting the sources of information. Spreading disinformation can amplify inaccurate information that often may benefit the wrong party.

Final Thoughts

Additionally, we wanted to make you aware that Bitdefender has announced an expanded partnership with the National Cyber Security Directorate in Romania where Bitdefender will offer both our consumer and business technology along with technical consulting and threat intelligence to any business, government institution, or private citizen in Ukraine for as long as necessary. We have also offered our business cybersecurity solutions to any business and government entity in a NATO or EU

country for one year if they have trust concerns regarding the current provider they may be using. You can read more here. If you know of any organization or individuals who could benefit from these offers, we'd appreciate your support to share this information with them.

MDR Actions Taken

1. Bitdefender is actively watching, researching, and identifying information that will be used to protect our customers' environments. We will continue to hunt for new indicators and monitor your environment 24x7.
2. Engage with your MDR service contact if any suspicious activity is detected and communicate questions or concerns through the customer success team.
3. Additionally, as indicators and malware are discovered, Bitdefender adds signatures to detect the activity in EDR tooling.

Recommendations

1. Phishing will continue to be the top way to target organizations, so beware. Some examples of phishing seen so far in the security community:
    a. Ukraine support to refugee evacuation
    b. Ukrainian national police criminal information targeted against specific individuals
    c. Sensationalist stories about seizing assets of those subject to sanctions
    d. Other relevant themes based on current events, such as cryptocurrency, COVID, regional or national elections, or similar
2. Inform users of security best practices and ensure tools, applications, and infrastructure are patched and backed up, if necessary.
3. Encourage users to contact security or IT support if they spot anything suspicious.
4. Monitor the news and update your threat models accordingly, and also inform employees if the threat posture changes.
5. Ensure that employees are aware of scams and social engineering which take advantage of the current war in Ukraine or related current events. These might include donation pages, solicitations for help, or phishing, as we've discussed above.
6. If your organization is at an increased risk of attack, ensure business continuity and incident plans are current, and have been recently rehearsed. Implement lessons learned and ensure the correct processes and procedures have been communicated to the applicable teams.

Additional References

1. https://businessinsights.bitdefender.com/security-advisory-a-risk-based-approach-for-improving-your-cybersecurity-posture-due-to-the-invasion-of-ukraine
2. https://www.bitdefender.com/ukraine.html?latest
3. https://dnsc.ro/citeste/press-release-dnsc-and-bitdefender-work-together-in-support-of-ukraine