IBM Security

Russia-Ukraine War Cybersecurity Resources

An Overview

X-Force Incident Command has been closely monitoring the cyber activity related to the Russian war in Ukraine. Our threat intelligence team has analyzed three different types of malware - the “Whispergate,” “Hermeticwiper/Partyticket” and “Isaacwiper” - which were used against Ukrainian, Lithuanian and reportedly Latvian organizations. The team is also monitoring a second potential DDoS attack against Ukrainian government websites. We have not seen any activity outside of those three countries thus far.

X-Force Threat Intelligence

X-Force is actively tracking and sharing the latest intelligence in the IBM X-Force Exchange Collection and will be updating the collection should additional information become available. The X-Force Exchange is the go-to place for the latest information about nation-state attacks so you can stay up to date on targets, techniques, and attack types.

The X-Force team also offers a portfolio of products and services that can help minimize your risk and impact of an attack. The services include:

X-Force Incident Response

– With X-Force IR’s 24x7 global Incident Response Emergency Support, you can stop attacks in progress, limit their impact, recover quickly, and reduce the risk of future incidents. The team also performs in-depth forensic analysis and malware reverse engineering to uncover every detail about the incident.

– With X-Force Active Threat Assessments, clients can learn if attackers are already inside their environment, what they may target and if it’s vulnerable. The engagement includes a report of what the X-Force threat hunting team found, how they found it and mitigation recommendations.

X-Force Red

– With its Application Security Services, X-Force Red assesses applications – whether they are pre-production or live – to find security flaws that attackers may leverage. The team offers code reviews (automated and manual), application vulnerability management services (scan and prioritize highest risk flaws), application penetration testing (hands-on, manual deep dive testing) and validated SAST/DAST scanning. These services can help find and fix application flaws that nation-state attackers may leverage.

– With its Penetration Testing Services, X-Force Red takes a deeper dive into your networks, applications, hardware, devices, and personnel to uncover high-risk vulnerabilities that only human attackers, not tools, can find and the team can show how attackers would leverage those flaws in a compromise. These services can help find and fix flaws that are potentially exposing your entire environment to nation-state attackers

– With its Vulnerability Management Services (VMS), X-Force Red can configure, deploy, and manage any enterprise class scanning solution, and prioritize the highest risk vulnerabilities that would enable a nation-state attack so that you know which to remediate first. The team also oversees the remediation process to confirm the flaws are fixed.

To learn more about X-Force services, visit ibm.com/xforce