JANUARY 26, 2022

Alert: State-Sponsored Cyber Threats

IMMEDIATE INTELLIGENCE & ACTIONABLE GUIDANCE

Nation-state actors often leverage the effects of cyber operations to achieve their strategic objectives on the world's stage.

— WHAT OCCURRED?

Both public and private organizations in Ukraine recently experienced a wave of cyber attacks, believed to originate from a nation-state, involving the disruption of government websites and the spread of malicious software, otherwise known as malware. While defacing websites is a more public attack, malware distribution is of greater concern because of its potential for creating widespread damage. While the incidents have so far been limited to Ukraine, this could be a precursor for increased malicious cyber activity across the U.S. and Europe.

— WHAT IS THE IMPACT?

Depending on the type of attack, the outcomes can involve financial loss, business interruption, compromised personal information, stolen sensitive data, unauthorized access of networks and databases, and reputational harm. Malware distribution has the potential for global impacts, similar to the NotPetya incident in 2017, which caused more than $10 billion in damages, according to an assessment from the White House.[1]

— WHO IS IMPACTED?

No organization or individual is off limits, especially when dealing with malware. Certain strains of malware have the ability to spread and infect networks and individuals who are not original targets of the cyber actors. Malware is naturally invasive and will continually search for new victims and infiltrate those without proper defenses.

— IMMEDIATE RECOMMENDATIONS

- Ensure multi-factor authentication is required to remotely access to your organization's network.
- Confirm software is up to date, prioritizing updates with known vulnerabilities.
- Validate appropriate controls are implemented if using cloud services.
- Remain vigilant regarding unusual network behavior and quickly determine if it's legitimate.
- Certify that antivirus and antimalware software is setup to protect your entire network.
- Monitor and isolate traffic from expected targets of these nation-state cyber attacks, such as organizations operating in Ukraine.
- Review incident response plans, including assigning specific individuals responsible for combating a live cybersecurity incident.
- Test and assess protocols for backing up vital data, including the restoration process, and confirm backups are separated from the main network.

(source: CISA)

— ISSUED ADVISORIES

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

- Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
- Alert: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

National Cyber Security Centre
a part of GCHQ

- Actions to Take When the Cyber Threat is Heightened

[1] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/j

How FTI Cybersecurity Can Help

We are a global team of cybersecurity experts with extensive experience hunting, identifying, and responding to advanced persistent threat (APT) actors at government and private organizations. Our team, capable of deploying worldwide, consists of dedicated cybersecurity experts, incident response consultants, developers, and data scientists with extensive investigative backgrounds. With our global team's deep experience in intelligence, law enforcement, and senior levels of government, **we maintain relationships with the top global intelligence agencies, regulatory authorities, and private agencies** to better support our clients in their prevention, response, and investigation of cyber threats and incidents. We can help by:

— **Holistic cybersecurity program assessment:** Ensure that existing policies and procedures are in place to handle an incident of this nature.

— **Vulnerability assessment and penetration testing:** Identify, evaluate, and prioritize securities weaknesses that may pose a risk to the security of your organization's network, applications, or services.

— **APT threat hunting services:** Ensure that the tactics, techniques, and procedures (TTPs) associated with this threat actor have not been employed within your network.

— **Understanding and assessing potential impact to your organization:** Analysis of systems and networks to determine if a cyber incident occurred, and if so, what was affected and how to properly proceed.

— **Independent expert investigative task force:** Rapid response and surge capabilities anywhere in the world, capable of unearthing key facts and data sets.

— **Incident Response:** Assist with containment, eradication, and recovery, including prohibiting data from leaving networks and preventing further damage.

ANTHONY J. FERRANTE
Senior Managing Director
Global Head of Cybersecurity
ajf@fticonsulting.com

JORDAN RAE KELLY
Senior Managing Director
Head of Cybersecurity, Americas
jordan.kelly@fticonsulting.com

KYUNG KIM
Senior Managing Director
Head of Cybersecurity, APAC
kyung.kim@fticonsulting.com

DAVE HARVEY
Managing Director, EMEA
United Kingdom
dave.harvey@fticonsulting.com

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.