SECURITYWEEK NETWORK:

- Cybersecurity News
- Webcasts
- Virtual Events

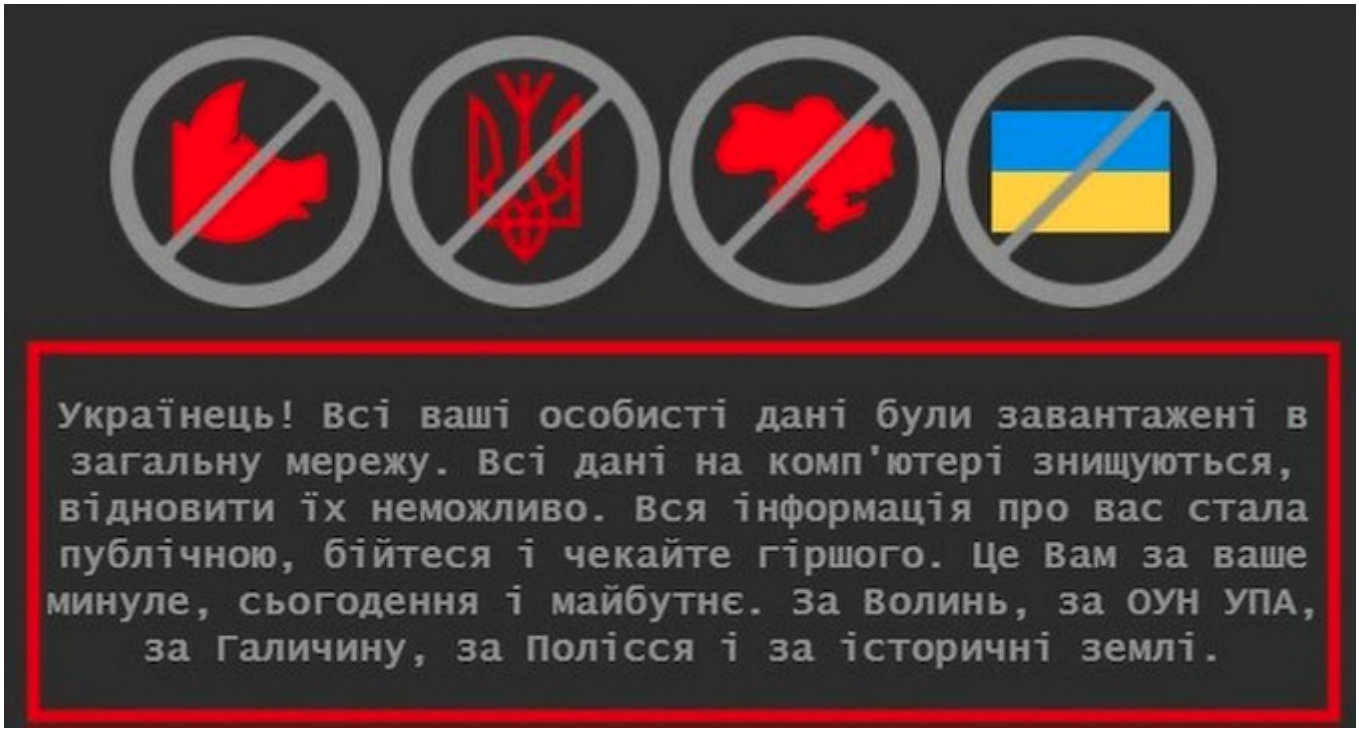
Security Experts:

WRITE FOR US

- Subscribe
- 2022 CISO Forum
- ICS Cyber Security Conference
- Contact
- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Supply Chain
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification

Ukraine Attacks Involved Exploitation of Log4j, October CMS Vulnerabilities

By Eduard Kovacs on January 19, 2022



CISA Warns Organizations of 'Critical Threats' Following Ukraine Attacks

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned organizations about "potential critical threats" following the recent cyberattacks aimed at Ukraine.

In a two-page "insights" document published on Tuesday, CISA advised all organizations — regardless of their size or sector — to immediately implement steps to reduce the likelihood of damaging breaches, quickly detect intrusions, ensure that they are prepared to respond to an intrusion, and improve their resilience to destructive attacks.

"This CISA Insights is intended to ensure that senior leaders at every organization in the United States are aware of critical cyber risks and take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise," CISA said.

Tens of Ukrainian government websites were hacked last week, being defaced with messages suggesting the attack was in response to the country's pro-Western stance. A majority of the sites have since been restored.

Russia has been blamed for the attack, but the Kremlin has denied the accusations, with the presidency claiming that "Russia has nothing to do with these cyberattacks."

Microsoft said the operation involved a new and destructive piece of malware that the tech giant tracks as WhisperGate. The malware has been described as a master boot record wiper disguised as ransomware —

WhisperGate appears to be ransomware, but it lacks a recovery mechanism for when victims pay the ransom.

An analysis of the malware conducted by Symantec showed that samples related to WhisperGate may have been deployed to unknown victims as early as October 2021.

The attackers breached Ukrainian government networks through a supply chain attack involving a third-party software supplier named Kitsoft, which has confirmed that its infrastructure had been compromised.

Ukrainian cybersecurity agencies said the attack involved exploitation of CVE-2021-32648, a vulnerability in the October CMS, as well as exploitation of the notorious Log4Shell flaw, and DDoS attacks.

The October CMS flaw allows attackers to gain access to accounts after resetting their password.

The October CMS vulnerability was added by CISA on Tuesday to its Known Exploited Vulnerabilities Catalog. Security holes added to this list must be patched by federal agencies within two weeks.

CISA's warning comes just days after several U.S. government agencies issued a joint advisory to provide an overview of cyber operations linked to Russia. The advisory was published as tensions mount over a potential Russian invasion of Ukraine.

On one hand, the recent attacks aimed at Ukraine add to tensions. On the other hand, Russia for the first time announced that it has arrested alleged members of a notorious ransomware gang at the request of the United States.

Related: Five Key Signals From Russia's REvil Ransomware Bust

Related: Ukraine Names Russian FSB Officers Involved in Gamaredon Cyberattacks

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

Ransomware Group Leaks Files Stolen From Cisco
Critical KEPServerEX Flaws Can Put Attackers in 'Powerful Position' in OT Networks
Cybersecurity M&A Roundup: 41 Deals Announced in August 2022
Hardcoded AWS Credentials in 1,800 Mobile Apps Highlight Supply Chain Issues
Ransomware Attacks Target Government Agencies in Latin America

Tags:

Cyberwarfare NEWS & INDUSTRY Virus & Threats Virus & Malware Malware Vulnerabilities

Most Recent Most Read

- Apple Warns of macOS Kernel Zero-Day Exploitation
- Google Completes $5.4 Billion Acquisition of Mandiant
- New Cyberespionage Group 'Worok' Targeting Entities in Asia

- SaaS Alerts Raises $22 Million to Help MSPs Protect Business Applications
- Ransomware Group Leaks Files Stolen From Cisco
- Ethical AI, Possibility or Pipe Dream?
- Vulnerability in BackupBuddy Plugin Exploited to Hack WordPress Sites
- Montenegro Wrestles With Massive Cyberattack, Russia Blamed
- Google Patches Critical Vulnerabilities in Pixel Phones
- Critical KEPServerEX Flaws Can Put Attackers in 'Powerful Position' in OT Networks

Popular Topics

Cybersecurity News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

Virtual Cybersecurity Events
Webcast Library
CISO Forum
ICS Cyber Security Conference
IT Security Newsletters
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Event Sponsorships
Writing Opportunities
Feedback
Contact Us

Wired Business Media