F#RTINET. **OUTBREAK ALERTS**

Russian Cyber Espionage Attack **Russia's Cyber Unit Targets Global Infrastructure**

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a CVEs: CVE-2020-1472,CVE-2021-26084,CVE-2021-3156,CVE-2021-4034,CVE-2022-27666,CVE-2021-33044,CVE-2021-33045,CVE-2022-26134,CVE-2021-3045,CVE-2

2022-26138,CVE-2022-3236

FortiGuard Labs continues to observe attack attempts exploiting the vulnerabilities highlighted in the recent CISA advisory about Russian military cyber actors. These actors are targeting U.S. and global critical infrastructure to conduct espionage, steal data, and compromise or destroy sensitive information.

Background Unit 29155 cyber actors are known to target critical infrastructure and key resource sectors, including the

Latest Developments

members, the EU, Central American, and Asian countries since 2020. CISA's analysis concluded Unit 29155 cyber actors had exploited multiple CVEs for initial access. These CVEs primarily involve remote code execution, authentication bypass, privilege escalation, and buffer overflow issues

government services, financial services, transportation systems, energy, and healthcare sectors of NATO

affecting products and software such as Dahua IP Cameras, Atlassian Confluence Server and Data Center, and Sophos Firewall Vulnerabilities. According to the advisory, to date, the FBI has observed more than 14,000 instances of domain scanning across at

least 26 NATO members and several additional European Union (EU) countries. Fortinet Customers remain protected by the FortiGuard IPS (Intrusion Prevention System) Security Service that

can detect and block exploit attempts targeting the vulnerabilities listed in the CISA's advisory and has protections against known malware used in the campaigns. Please see the Solution Tab for full list of available protections.

https://www.fortiguard.com/threat-signal-report/5197/

since 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

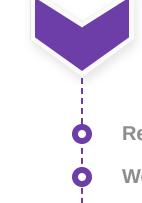
September 5, 2024: CISA released a joint advisory as a collective assessment of Unit 29155 cyber operations

August 21, 2024: CISA recently added two new vulnerabilities related to CVE-2021-33044, CVE-2021-33045 (Dahua IP Security Cameras) to thier Known Exploited Vulnerabilities Catalog.

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

PROTECT

June 14, 2023: FortiGuard Labs released a Threat Signal on the related campaigns.



Reconnaissance

Weaponization

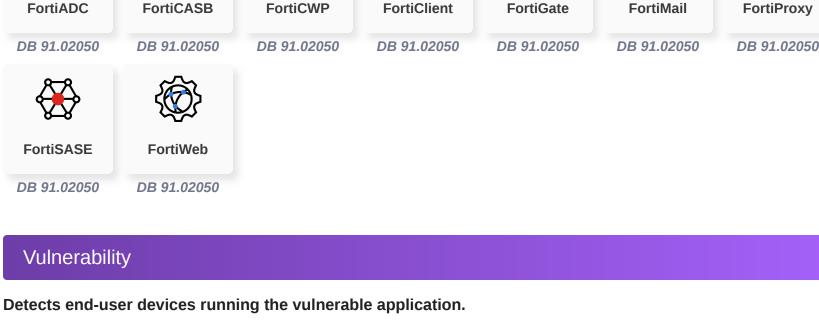
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity

Delivery

AV

FortiADC FortiCASB FortiCWP

Detects known malware related to the Outbreak



AV (Pre-filter)

DB 91.02050

DB 28.859

FortiClient

DB 2.355

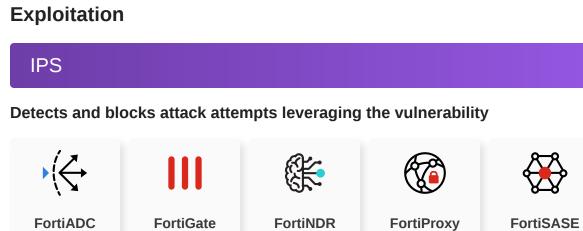
FortiEDR FortiNDR FortiSandbox

DB 91.02050

DB 28.859

FortiWeb

Detects known malware related to the Outbreak



DB 28.859

DB 28.859

DB 28.859

DB 91.02050

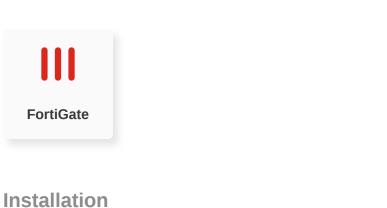
DB 0.00333 DB 1.00036

FortiADC

Web App Security

IoT/IIoT Virtual Patch

Detects and blocks attack attempts leveraging the vulnerability



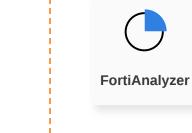
DETECT

alert and generate reports:

C2

Action

IOC



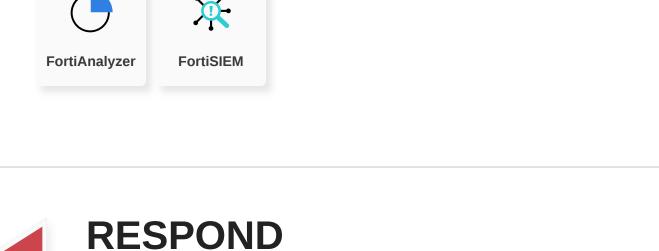
Outbreak Detection

Threat Hunting

FortiSOCaaS

FortiNDR FortiClient FortiSIEM FortiSOAR FortiAnalyzer Cloud DB 613 v7.4

Find and correlate important information to identify an outbreak, the following updates are available to raise



Develop containment techniques to mitigate impacts of security events:

FortiSIEM



Response

RECOVER

NOC/SOC Training

End-User Training

and other forms of cyberattacks.

(and recovery from) security incidents:

Response

Readiness

Assisted Response Services

Automated Response

FortiXDR

Services that can automaticlly respond to this outbreak.

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



NSE Training

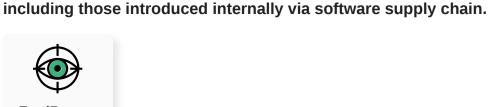
IDENTIFY

Identify processes and assets that need protection: **Attack Surface Hardening**

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download

Improve security posture and processes by implementing security awareness and training, in preparation for



FortiDAST

Attack Surface Monitoring (Inside & Outside)

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government

Security reconnaissance and penetration testing services, covering both internal & external attack vectors,



MITRE: WhisperGate

Justice.gov

FortiRecon: **EASM Vulnerability Management**

Security

Rating

FortiClient



https://attack.mitre.org/software/S0689/

Learn more about FortiGuard Outbreak Alerts