Wildix

The Burning Bear Problem: Russia's Unrestricted Cyberwarfare

The Burning Bear Problem

The use of cyberwarfare as part of a wider information war by the Russian state, emphasizing destabilization, destruction and widespread issues for non-military and non-governmental targets.

11 Years of Russia-Supported Cyberterrorism

2011	OECD warns of growing arsenals of **military cyberweapons**. Just-in-time infrastructure is vulnerable, notably food suppliers and manufacturers.
2012	Vladimir Putin is elected as president of Russia for a second nonconsecutive tenure.
2013	Snake virus targets Ukrainian government systems, designed to create disruption before the occupation of Donbas and Crimea.
2014	U.S. government agencies are hit by repeated attacks from Cozy Bear, and Ukraine's electoral system is hit by a sustained cyberattack aimed at disrupting its elections.
2015	German and French governments have information stolen during Russian cyberattacks. Hack of the DNC results in a sensitive information leak.
2016	Poland comes under a three-year disinformation campaign carried out by Russian cyberwarfare groups.
2017	Further cyberwarfare attacks on Ukraine. NATO starts unraveling Russian cyberwarfare doctrine.
2018	South Korea: Winter Olympics come under sustained cyberattacks from Russia-linked groups that disable Olympic IT infrastructure.
2019	Fresh cyberattacks against Georgia through the GRU's Sandworm division. 15,000 websites go offline.
2020	SolarWinds hack results in data being compromised at the US Pentagon, the Department of Homeland Security and thousands of other organizations.
2021	Russia-based cyberattacks involving ransomware peak, with well-publicized attacks on Colonial Pipeline and meat supplier JBS. Shortages of oil and food in the United States.
2022	War in Ukraine begins. Western support is unprecedented, despite Russian threats.

State-Sponsored Cyberterrorism

Russia has many opportunities for cyberhackers. In a nation where there are numerous developers but few jobs and a devalued rouble, these educated professionals flock to organizations that let them make significant wealth.

And Russian intelligence has taken advantage of that.

The result: Unprecedented information theft, disruption and monetary loss.

Russia sees cyberwarfare as part of its information warfare strategy. As a result, it doesn't use the term cyberwarfare (roughly kibervoyna) unless it's translating western discussion of the topic. As a philosophy, it means that cyberwarfare is a legitimate domination strategy even when it's technically at peace with a nation — and even against Russians who the government considers disruptive.

"Why do we need a world if Russia is not in it?"

Russian state TV presenter
Dmitry Kiselyov
February 28, 2022

Rather than seeing these as military operations, Russia considers them part of its pre-war strategy and even similar to the way the western world sees sanctions. And the use of non-state actors helps it to distance these cyberwarfare acts from its official military activities. The free flow of information is considered a threat to Russian interests; this can be seen through the increasingly repressive laws the country has used in recent weeks.

And anything is a valid target for these "non-state actors" — which, it turns out, are nearly always associated with either the FSB (Russia's federal security service) or the GRU (Russia's military intelligence):

Hospitals have been extensively targeted by the FIN12 hacking group, using a weakness in a Citrix environment to deploy ransomware that puts lives at risk.

Mandiant *October 7, 2021*

Numerous schools in the UK, Canada and the United States have been targeted using a combination of phishing attacks and targeted vulnerabilities in VPNs (including Citrix, Fortinet and Palo Alto). However, most cyberattacks are through Remote Desktop Protocol using stolen credentials.

National Cyber Security Center *June 4, 2021*
CYDEF *January 25, 2021*
AP News *February 1, 2022*

The Russian hacker group Cl0p hit the UK's Police National Computer database. It attacked a third-party company that was handling the data, creating what's called a supply-chain attack.

TechMonitor *December 20, 2021*

French software firm Centreon was breached by GRU-linked Sandworm, compromising data related to Airbus, the French Ministry of Justice and nuclear power plant operator EDF.

Politico *February 15, 2021*

Aviation networks are particularly vulnerable, relying on real-time data exchange to safely guide large numbers of aircraft across densely congested airspace, and the CISA notes that Russian hackers target hubs regularly.

CISA *January 11, 2022*

Is Your Business a Target?

Russian military doctrine states that all entities within a non-aligned country are valid targets.	Hacker groups have moved from targeting large enterprises with good security to targeting smaller suppliers, businesses and even nonprofits with weaker security.	74% of all ransomware revenue in 2021 ended up in Russia, worth $400 million. *Chainalysis February 14, 2022*

Cyberattacks are among the most destructive forms of attack on a business. They lock up the data in target computers, making it nearly impossible to recover. This alone can have a severe, long-term impact on operations. It can be worse, however.

83% of 2021's ransomware attacks involved lockouts and data extraction, instead of a simple lockout.

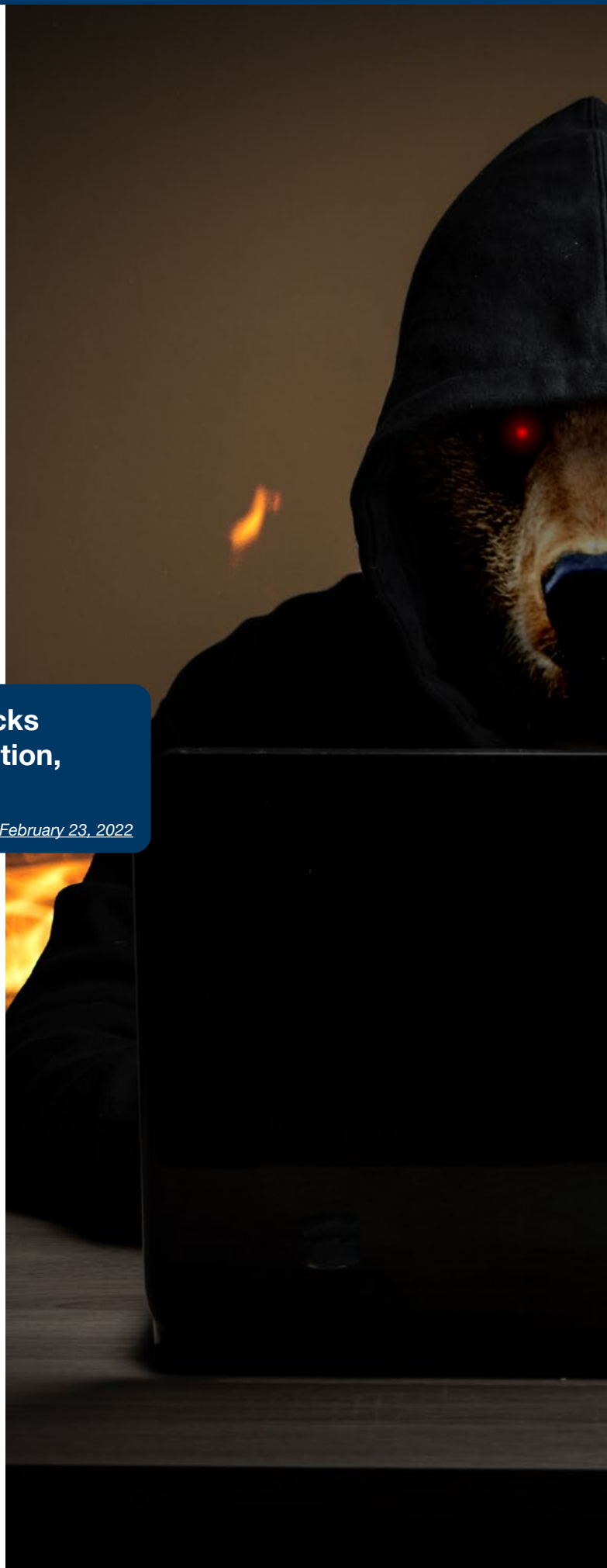
Venafi February 23, 2022

Any form of malware can wreak havoc. When Maersk, the global shipping and transport company, was hit by an attack, it had to:

- Replace 49,000 laptops
- Rebuild 1,000 applications
- Recover 200 applications
- Scrap 3,500 servers
- Recover all Outlook contacts from clients, contractors, customers and employees

CxO Hub August 2019

This is a classic result of the Burning Bear problem: The NotPetya malware that struck Maersk was simply designed to destroy, and it didn't care who it hit — as long as it wasn't Russian.



Mitigating the Burning Bear Problem

Most cyberattacks focus on three pressure points:

1. Distributed denial of service attacks
2. Exploitation of human error, such as through phishing
3. Exploitation of software vulnerabilities

Vulnerabilities are often exploited in these products:

FortiGate VPNs, Cisco routers, Oracle WebLogic Server, Kibana, Zimbra software, Exim SMTP, Pulse Secure, Citrix, Microsoft Exchange, VMWare, F5 Big-IP, Oracle WebLogic

CISA January 11, 2022

But this list is nowhere near comprehensive.

Any legacy software, client or equipment could be used to destroy infrastructure and put lives at risk. And the scorched-earth policy that Russia follows shows that the Burning Bear problem is very real.

We know that you need serious security when it comes to data. And having easily- compromised systems should never happen — imagine what criticism you'd face if it transpired you had an outdated system that created a major data breach for a client.

That's why we recommend replacing your legacy PBX with a cloud PBX every time.

Benefits include:

- Rapid updates
- Secure servers
- No data held outside your region
- No downloads required
- No connections with Russia

This is the least you need to help your business and your nation to stay secure. So whether you choose Wildix or another cloud PBX provider, talk to us today to discover the possibilities.

“The target of the first cyberattack by Russia is unknown. However, it wasn’t the last.”

- Dimitri Osler, CTO of Wildix

Wildix

www.wildix.com