**[Cyber-Safe](http://money.cnn.com/technology/cyber-safe/)**

# **Global cyberattack: What you need to know**

**By Selena Larson and Jethro Mullen   @CNNMoney**

**June 28, 2017: 6:46 AM ET**

**A massive ransomware attack has hit businesses around the world, causing major companies to shut down their computer systems.**

Researchers are still investigating the software behind the attack, warning that it's more sophisticated than the WannaCry worm that struck hundreds of thousands of computers across the globe last month. "WannaCry was a tremendous failure. It was a lot of noise, very little money, and everyone noticed it," said Craig Williams, an expert at cybersecurity firm Cisco Talos. "What we're seeing today is a much more intelligent worm." Big global brands -- like Mondelez (MDLZ), the maker of Oreos, and British advertising giant WPP (WPPGF) -- say their IT systems are experiencing problems.

**What does it do?**

The ransomware infects computers and locks down their hard drives. It demands a $300 ransom in the anonymous digital currency Bitcoin. The email account associated with the ransomware has been blocked, so even if victims pay, they won't get their files back. Law enforcement and cybersecurity experts agree that victims should never pay ransoms for such attacks.

**Who's been hit?**

Top international businesses headquartered in Europe and the U.S. have come under attack. They include Russian oil and gas giant Rosneft, Danish shipping firm Maersk, U.S.-based pharmaceutical company Merck and law firm DLA Piper. French retailer Auchan Group and the real estate division of BNP Paribas were also affected. Ukrainian organizations took a particularly heavy blow. Banks, government offices, the postal service and Kiev's metro system problems, officials said. The ransomware also caused problems with the monitoring system of the Chernobyl nuclear power plant.

**Am I vulnerable?**

Regular consumers who have up-to-date Windows computers are safe from this attack, experts say. However, if there's one out-of-date machine on a company's network, it could infect other connected computers.

**Where did it start?**

Researchers are still figuring out exactly what happened. But Cisco Talos says one way the ransomware got into computer systems was through software in Ukraine, a country that was hit especially hard by the attacks.

**Who's behind it?**

It's still too early to say who might be responsible for unleashing the virus. Intelligence agencies and security researchers have linked last month's WannaCry attack to a group associated with North Korea. But it's unclear if the new ransomware worm is connected.

**How is this different from WannaCry?**

Like WannaCry, the new ransomware attack uses the EternalBlue tool to spread. But researchers say it also uses other parts of Windows to infect computers, including seizing user credentials.

Unlike WannaCry, it locks down a computer's entire hard drive instead of just the files. And it didn't shoot across the internet the way WannaCry did -- instead, it spreads inside company networks.

"It seems that the ones in charge of this campaign have learned quite a lot from the WannaCry campaign," said Itay Glick, the CEO of Israeli cybersecurity company Votiro.

*-- Alec Macfarlane, Omar Khan, Anish Gawande, Victoria Butenko and Bex Wright contributed to this report.*

CNNMoney (San Francisco) First published June 28, 2017: 2:00 AM ET

<http://money.cnn.com/2017/06/28/technology/ransomware-attack-petya-what-you-need-to-know/index.html>

PREDICTING – OBSERVAR OS DETALHES E RESPONDER (O QUE O TEXTO IRÁ TRAZER?)

LEITURA DAS PALAVRAS COGNATAS

OBSERVAR SE TEM FALSOS COGNATOS

INFERIR PALAVRAS DESCONHECIDAS ATRAVÉS DO CONTEXTO

OBSERVAR AS PERGUNTAS

Empresas em vários países foram alvo de mais um grande ataque cibernético nesta terça-feira 27 de junho de 2017. Quem tentou sacar dinheiro de caixas eletrônicos na [Ucrânia](http://g1.globo.com/tudo-sobre/ucrania/) foi saudado com uma mensagem dos hackers, exigindo o equivalente a R$ 1 mil para ter acesso à conta bancária. Lá o vírus se espalhou tanto que já é considerado o pior ataque cibernético da história do país. Até a usina nuclear desativada de Chernobyl foi atingida. Os testes de radiação, que são constantemente realizados de forma eletrônica, estavam sendo feitos manualmente. O site e o painel de voos do aeroporto da capital, Kiev, saíram do ar e dezenas de voos atrasaram. Os ataques se alastraram também pela Rússia, Noruega, Romênia, Espanha, Holanda, Reino Unido e Estados Unidos. O Departamento de Segurança Interna americano está monitorando a ameaça. Nos Estados Unidos, pelo menos duas empresas - uma do setor farmacêutico e um escritório de advocacia multinacional – declararam ter sido alvo dos hackers.

Este novo ataque cibernético causa problemas pois

1. utiliza suas senhas para poder ter acesso a sua conta.
2. faz *back up* de todos os seus arquivos e deleta.
3. bloqueia seu computador e hackers pedem dinheiro para desbloquear.
4. bloqueia seu hd e faz com que você deposite na conta do hacker para obter acesso novamente.

<http://g1.globo.com/jornal-nacional/noticia/2017/06/novo-ataque-cibernetico-atinge-bancos-aeroportos-e-ate-chernobyl.html>