

Still crying over WannaCry, Petya and Goldeneye? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/still-crying-over-wannacry-petya-and-goldeneye>

Details:

Summary

This blueAPACHE post reports: Even as organisations continue to cope with last month's wave of ransomware attacks linked to WannaCry, on Tuesday, the world woke up to yet another global ransomware outbreak. Victims of the latest Petya ransomware include the Ukrainian government, the Chernobyl nuclear radiation monitoring system, U.S. It concerns emPOWER Security, Managed Detection & Response, Offsite Backup as a Service. Published in 2017. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2017
Services referenced	emPOWER Security, Managed Detection & Response, Offsite Backup as a Service
Topic	Still crying over WannaCry, Petya and Goldeneye?

Article

Even as organisations continue to cope with last month's wave of ransomware attacks linked to WannaCry , on Tuesday, the world woke up to yet another global ransomware outbreak. Victims of the latest Petya ransomware include the Ukrainian government, the Chernobyl nuclear radiation monitoring system, U.S. pharmaceutical company Merck, Russian steel and mining firms and many others. Similar to WannaCry, Petya exploits the Windows SMBv1 vulnerability on unpatched computers. However, unlike WannaCry, which spread through email phishing campaigns, Petya is more traditional – the initial infection vector is associated with a software update for a Ukrainian tax accounting program – and has the capacity to spread rapidly throughout the network, infecting even those computers that have already been patched. Now, more than ever before, it is imperative that organisations are able to detect and respond to security events in a prompt manner. There is no substitute for good defences – they are a must. But even with the most advanced security measures there are limitations. It doesn't matter how good your firewalls are, or how good your Intrusion Detection / Prevention System (IDS/IPS) is – you will be compromised at some point. It is understanding your security limitations, and preparing for them, that makes the difference in whether or not you can survive a cyberattack. So what can you do to protect yourself?

Vulnerability Scanning – Keep yourself up-to-date with known areas of weakness in your systems. One of the major concerns with such attacks is that many organisations do not know they have been infected until it is far, far too late. The first indication they receive is when critical files and data are already unavailable and being held hostage. But it does not have to be that way. Attacks such as these

are rarely 'quiet'. They tend to be loud and noisy if you know where to look and what to look for. Traditionally, the real time analysis of system, server and application logs has been time consuming, involved and difficult. Logs were only looked at for after-event analysis. But to stay ahead of security incidents, organisations need a way of identifying what is occurring, and where it is occurring, in real time. This is where Security Incident and Event Monitoring (SIEM) can help. A SIEM platform can correlate and analyse security event data from across your cloud and on-premises environments in real time. This helps identify the source of compromise, contain it by isolating the infected systems and then implement mitigating actions – all in a timely manner that can limit damage.

Patching – Stay on top of patch management to limit attack vectors Continuing to run critical services on an unsupported or unpatched system carries an extreme risk. Without regular security patches and updates, your systems become a playground for hackers who are constantly on the lookout for exactly such vulnerabilities to exploit.

Backups – Maintain regular and frequent backups of all critical data and systems When all else fails, nothing can take the edge off a ransomware attack than knowing that all your critical systems and data are securely backed up and can be restored. Ideally your data backups should be maintained on external devices and stored offline and offsite. As a final note, according to reports, the email address that was being used to communicate with Petya victims has now been suspended, which means that even when the ransom is paid, there is no way to receive the decryption keys and retrieve files. There has been no impact of this outbreak on blueAPACHE clients. If you have concerns or want to improve your organisation's security posture, contact the blueAPACHE security team . Our security consultants can assess your organisation's level of exposure to phishing attacks and conduct workshops to educate your staff.

Related

emPOWER Security

emPOWER Security (pillar)

Managed Detection & Response

Offsite Backup as a Service

emPOWER Cloud (pillar)

Frequently asked questions

Which organisations does the article name as victims of the Petya ransomware outbreak?

The article names the Ukrainian government, the Chernobyl nuclear radiation monitoring system, US pharmaceutical company Merck, and Russian steel and mining firms among Petya's victims.

How did Petya's initial infection method differ from WannaCry's, according to the article?

The article says Petya's initial infection vector was a compromised software update for a Ukrainian tax accounting program, whereas WannaCry spread through email phishing campaigns; both then exploited the Windows SMBv1 vulnerability to spread.

What three protective measures does the article recommend against ransomware?

The article recommends vulnerability scanning to stay aware of system weaknesses, patch management to limit attack vectors, and maintaining regular, offline and offsite backups of critical data and systems.

What does the article say happened to the Petya ransom payment channel?

The article says reports indicated the email address used to communicate with Petya victims was suspended, meaning even victims who paid the ransom had no way to receive decryption keys.

Is the information in this post still current?

No. It reports the 2017 WannaCry and Petya ransomware outbreaks; for blueAPACHE's current ransomware and incident response guidance, see the emPOWER Security pillar page rather than this post.

Source

<https://www.blueapache.com/blog/still-crying-over-wannacry-petya-and-goldeneye/>

Knowledge Base

How did Petya's method of spreading differ from WannaCry's?

Like WannaCry, Petya exploits the Windows SMBv1 vulnerability on unpatched computers, but unlike WannaCry, which spread through email phishing campaigns, Petya's initial infection vector was associated with a software update for a Ukrainian tax accounting program, and it could spread rapidly throughout a network, infecting even already-patched computers.

What happened to the ransom payment process for Petya victims, ?

According to reports cited in the article, the email address used to communicate with Petya victims was suspended, meaning that even if victims paid the ransom, there was no way to receive the decryption keys and retrieve their files.

Were any your clients affected by the Petya ransomware outbreak?

there was no impact of the Petya outbreak on our clients.