Client Update
Petya Ransomware Attacks

WASHINGTON, DC
Luke Dembosky
ldembosky@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore
jjpastore@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

LONDON
Jane Shvets
jshvets@debevoise.com

Robert Maddox
rmaddox@debevoise.com

HONG KONG
Mark Johnson
mdjohnson@debevoise.com

MOSCOW
Anna V. Maximenko
avmaximenko@debevoise.com

On June 27, 2017, a new wave of ransomware attacks quickly spread across the globe. The “Petya” malware encrypts and holds for ransom the entirety of an infected computer. Initial reports suggested that the malware targeted Ukrainian public infrastructure. Public and private entities in Russia, the EU, and the U.S. now reportedly have been affected. Like the recent WannaCry attacks, Petya is a reminder of the advisability of addressing ransomware as part of a broader cybersecurity program.

WHAT HAPPENED?

The initial intrusion appears to come through a malicious email attachment. The malware then exploits the same vulnerability targeted by WannaCry . Any computers that were unpatched following the WannaCry attacks thus remain vulnerable to Petya. Petya also attempts to harvest administrative credentials and spread horizontally through a compromised network.

Petya reboots the victim’s computer and encrypts the master file table, rendering the entire system inoperable. This differs from previously observed malware that targeted individual files.

WHAT TO DO?

Our suggestions for action in the wake of Petya track our recent recommendations regarding WannaCry. Briefly: Above all, patch your systems directly at Microsoft’s website. Go there directly. Ignore any unsolicited email you may have received that claims to offer a patch. Also, remember that even if you are able to unlock your files, the underlying malware will remain on the machine. Steps should be taken to eradicate it.

Consider also regularly backing up your data—and, just as important, testing your ability to actually operate from the backups. Remind employees to take special care not to click on unknown email attachments. Assess whether your technical defenses include current tools. Examples include: updated antivirus at system endpoints; firewalls to filter malicious traffic; network segmentation to stop or slow the spread of infection; and intrusion detection software to provide timely alerts of unusual traffic in your network. It is also prudent to line up outside help before any incident. This includes picking vendors (yes, including a law firm), and building law enforcement relationships.

We increasingly see specific ransomware preparations included in our clients' "tabletop" cyber response drills. Written incident response plans also increasingly address ransomware. Check your cyber coverage to see how a ransomware incident might or might not be covered. Collect and share threat intelligence through an Information Sharing and Analysis Center or similar cross-industry or multi-sector organization.

If you do get hit with a ransomware attack, legal as well as technical responses may be called for. The disruption that an attack can cause may trigger contractual or regulatory notifications. Consult counsel regarding the potential legal and practical ramifications of the decision whether to pay the ransom.

What Next?

Petya's quick global spread suggests that post-WannaCry patching is, for many, still a work in progress. Regulators consider effective patch management a critical part of a risk-based information security program. Internal counsel can mitigate cybersecurity and regulatory risks by refreshing discussions surrounding ransomware and patch management with their information security counterparts. This can also calm executive concerns.

* * *

For questions or assistance, please do not hesitate to call on any member of the Debevoise Cybersecurity & Data Privacy global practice team.