Cynet
Advanced Threat Detection & Response

CYNET SECURITY REPORT: STOPPING NOTPETYA IN ITS TRACKS

DEADLIER THAN WANNACRY

Security researchers around the world are calling June 27th's Petya attacks deadlier than WannaCry. The malicious ransomware, which has been around since 2016, resurfaced with a vengeance, hitting companies in Europe and the US, and spreading swiftly – halting operations and demanding Bitcoin ransom.

If your organization was one of the infected, the odds are low on returning your data – unless you backed up your valuable information. Email provider Posteo has closed the account the ransomware vandals were giving victims to contact for keys. So if WannaCry was not a lesson in backing up, maybe this will be.

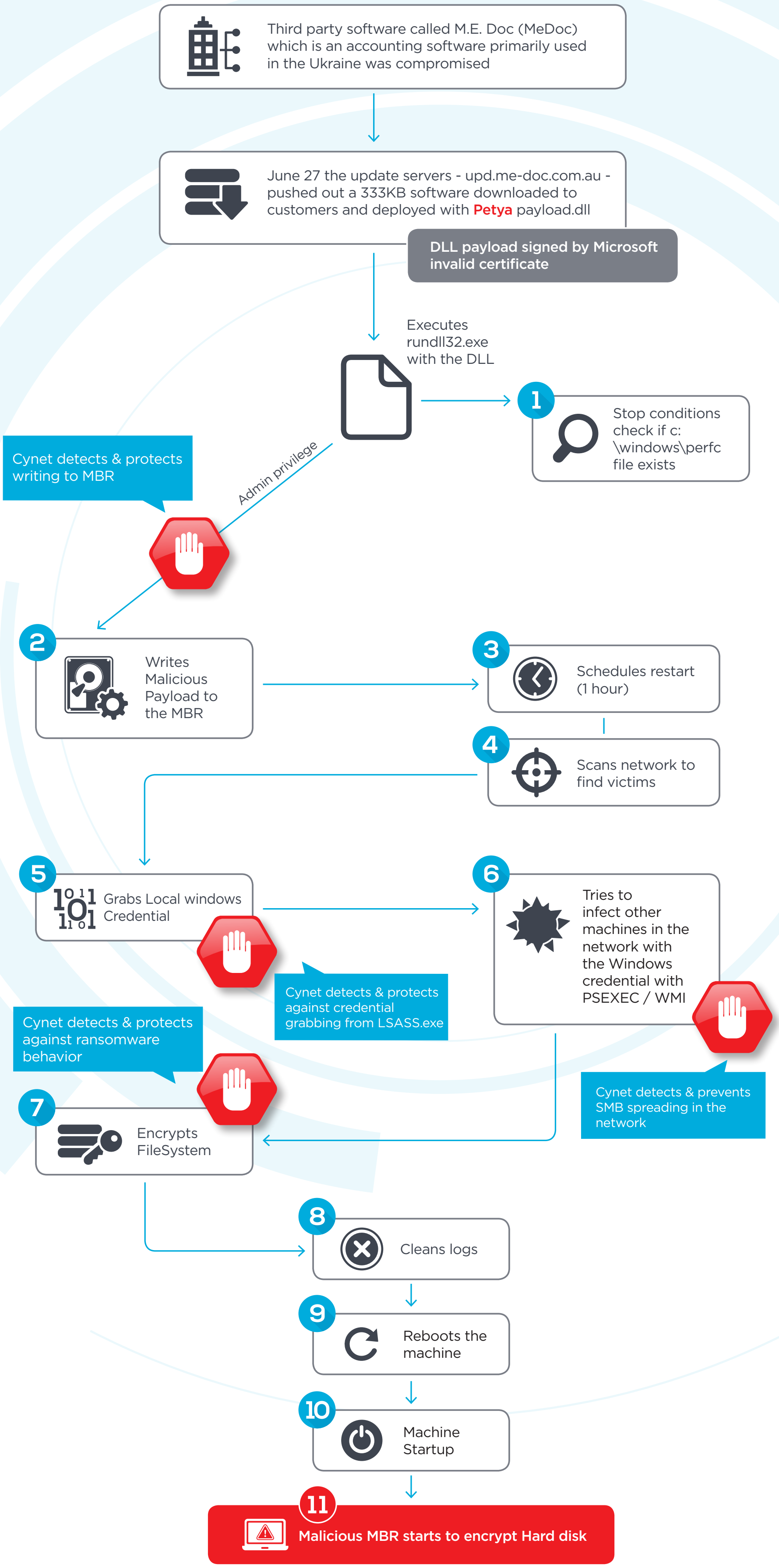
SPREADING LIKE WILDFIRE

Original reports focused heavily on Ukraine, as the initial attacks took place via a built-in update included in a program used by companies working with the Ukraine government. Industries hard hit in the Ukraine included finance, utilities and transportation, in addition to government offices. Within hours, Petya had spread to some 2,000 organizations in Spain, the UK, the Netherlands, France, the US and other countries.

HOW IT WORKS

The latest estimates list ransom damages around $9000, not a lot considering the rate with which the attack has spread. Like WannaCry, Petya takes advantage of the same NSA hacked EternalBlue exploit. But unlike WannaCry, which encrypted individual files, Petya focuses on an organization's administrator tools. The hacked computers are rebooted and the hard disk'sMFT is encrypted, effectively infecting the MBR, putting it out of commission and blocking system access.(And if this does not work, it can also just encrypt files like your usual ransomware.) Malicious code is injected into the MBR and the unlucky victim's find themselves staring at a black screen with red text, demanding a payment of 300 dollars in ransom.

CYNET MITIGATION LAYERS



Third party software called M.E. Doc (MeDoc) which is an accounting software primarily used in the Ukraine was compromised

June 27 the update servers - upd.me-doc.com.au - pushed out a 333KB software downloaded to customers and deployed with **Petya** payload.dll

DLL payload signed by Microsoft invalid certificate

Executes rundll32.exe with the DLL

1 Stop conditions check if c:\windows\perfc file exists

Admin privilege

Cynet detects & protects writing to MBR

2 Writes Malicious Payload to the MBR

3 Schedules restart (1 hour)

4 Scans network to find victims

5 Grabs Local windows Credential

Cynet detects & protects against credential grabbing from LSASS.exe

6 Tries to infect other machines in the network with the Windows credential with PSEXEC / WMI

Cynet detects & prevents SMB spreading in the network

Cynet detects & protects against ransomware behavior

7 Encrypts FileSystem

8 Cleans logs

9 Reboots the machine

10 Machine Startup

11 **Malicious MBR starts to encrypt Hard disk**

Cynet stops Petya. We stop the infection and encryption of the host. We do this by protecting the Master Boot Record, and by detecting malicious SMB connections originating from suspicious files, stopping spread of the ransomware. Over the course of the June 27th attacks, while the much of the word was going into system lockdown in an effort to contain damages, Cynet customers were able to rest easy, knowing the Cynet 360 platform had their assets covered. The Cynet 360 advanced threat detection and response platform is the only effective, holistic option available for the organization looking to ensure the highest level of security, while truly simplifying their IOCs detection and response.

360°
CYNET PLATFORM

HOW CYNET PROTECTS ITS CUSTOMERS

1. **Protects** host from infection
2. **Defends** host from encryption
3. **Stops** the Ransomware distribution